

日本国特許庁

PATENT OFFICE  
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
in this Office.

出願年月日  
Date of Application:

1998年 7月16日

願番号  
Application Number:

平成10年特許願第201497号

願人  
Applicant(s):

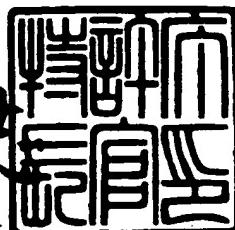
ソニー株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

1999年 5月21日

特許庁長官  
Commissioner  
Patent Office

伴佐山 建志



【書類名】 特許願  
【整理番号】 9800693304  
【提出日】 平成10年 7月16日  
【あて先】 特許庁長官殿  
【国際特許分類】 G06F 12/14  
【発明の名称】 情報処理装置および情報処理方法  
【請求項の数】 10  
【発明者】  
【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社  
内  
【氏名】 日下部 進  
【発明者】  
【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社  
内  
【氏名】 高田 昌幸  
【発明者】  
【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社  
内  
【氏名】 佐々木 将央  
【特許出願人】  
【識別番号】 000002185  
【氏名又は名称】 ソニー株式会社  
【代表者】 出井 伸之  
【代理人】  
【識別番号】 100082131  
【弁理士】  
【氏名又は名称】 稲本 義雄  
【電話番号】 03-3369-6479

【手数料の表示】

【予納台帳番号】 032089

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9708842

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理装置および情報処理方法

【特許請求の範囲】

【請求項1】 データを記憶するデータ記憶手段と、

前記データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報を記憶する管理情報記憶手段と、

前記管理情報に基づいて、前記データ記憶手段を管理する管理手段と

を備えるデータ記憶装置に対して、前記管理情報を提供するための処理を行う情報処理装置であって、

前記管理情報を作成する作成手段と、

前記管理情報を暗号化する暗号化手段と

を備えることを特徴とする情報処理装置。

【請求項2】 前記管理情報が改竄されたか否かをチェックするためのチェックコードを演算する演算手段をさらに備え、

前記暗号化手段は、前記管理情報とともに、前記チェックコードも暗号化することを特徴とする請求項1に記載の情報処理装置。

【請求項3】 暗号化された前記管理情報を、所定の伝送媒体を介して、前記データ記憶装置に送信する送信手段をさらに備えることを特徴とする請求項1に記載の情報処理装置。

【請求項4】 前記管理手段が、前記データ記憶手段の記憶領域を階層構造にして管理する場合において、

前記暗号化手段は、親の階層の前記管理情報に含まれる前記キーを用いて、その子の階層の前記管理情報を暗号化することを特徴とする請求項1に記載の情報処理装置。

【請求項5】 データを記憶するデータ記憶手段と、

前記データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報を記憶する管理情報記憶手段と、

前記管理情報に基づいて、前記データ記憶手段を管理する管理手段と

を備えるデータ記憶装置に対して、前記管理情報を提供するための処理を行う

情報処理方法であって、

前記管理情報を作成する作成ステップと、

前記管理情報を暗号化する暗号化ステップと  
を備えることを特徴とする情報処理方法。

【請求項6】 データを記憶するデータ記憶手段と、

前記データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報を記憶する管理情報記憶手段と、

前記管理情報に基づいて、前記データ記憶手段を管理する管理手段と  
を備える情報処理装置であって、

暗号化された前記管理情報を受信する受信手段と、

暗号化された前記管理情報を復号する復号手段と、

前記管理情報を、前記管理情報記憶手段に記憶させる記憶制御手段と  
を備えることを特徴とする情報処理装置。

【請求項7】 前記管理情報が改竄されたか否かをチェックするチェック手段をさらに備える

ことを特徴とする請求項6に記載の情報処理装置。

【請求項8】 前記受信手段は、暗号化された前記管理情報とともに、その管理情報を改竄されたか否かをチェックするためのチェックコードも受信し、

前記チェック手段は、前記チェックコードに基づいて、前記管理情報が改竄されたか否かのチェックを行う

ことを特徴とする請求項7に記載の情報処理装置。

【請求項9】 前記管理手段が、前記データ記憶手段の記憶領域を階層構造にして管理しており、

前記管理情報が、その親の階層の管理情報を含まれる前記キーを用いて暗号化されている場合において、

前記復号手段は、暗号化された前記管理情報を、前記管理情報記憶手段に記憶されている、その親の階層の管理情報を含まれる前記キーを用いて復号する

ことを特徴とする請求項6に記載の情報処理装置。

【請求項10】 データを記憶するデータ記憶手段と、  
前記データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報を記憶する管理情報記憶手段と、  
前記管理情報に基づいて、前記データ記憶手段を管理する管理手段と  
を備える情報処理装置の情報処理方法であって、  
暗号化された前記管理情報を受信する受信ステップと、  
暗号化された前記管理情報を復号する復号ステップと、  
前記管理情報を、前記管理情報記憶手段に記憶させる記憶制御ステップと  
を備えることを特徴とする情報処理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報処理装置および情報処理方法に関し、例えば、IC (Integrated Circuit) カードを回収しなくても、その内蔵するメモリを管理するための管理情報を、安全に、追加したり変更したりすることができるようにする情報処理装置および情報処理方法に関する。

【0002】

【従来の技術】

例えば、電子マネーシステムやセキュリティシステムなどの利用が期待されているICカード（スマートカード）が開発されている。

【0003】

ICカードは、各種処理を行うCPUや、処理に必要なデータなどを記憶するメモリを内蔵しており、所定のリーダ／ライタ（R／W）に電気的に接触させた状態で、または電磁波を利用して非接触で、データの送受信が行われる。なお、R／Wとの間で、電磁波を利用して非接触でデータの送受信を行うICカードには、一般に、その電磁波により、必要な電力が供給される。

【0004】

【発明が解決しようとする課題】

ICカードを、例えば、電子マネーシステムやセキュリティシステムなどで利

用する場合においては、データの隠匿性や、ICカードの偽造を防止すること等のセキュリティが重要であり、一般には、システムの管理者（運用者）によって与えられるキーによって、ICカードに対するアクセスが可能となる。即ち、キーを有しない者のICカードへのアクセスは制限される。

#### 【0005】

また、例えば、接触式のICカードの標準を規定するISO（International Organization for Standardization）7816などでも、セキュリティについて規定されており、これによれば、ディレクトリまたはフォルダに相当するDF（Dedicated File）に鍵をかけることで、そのDFの階層に属するDFや、ファイルに相当するEF（Elementary File）へのアクセスが制限される。

#### 【0006】

ところで、ICカードに対して、新サービスを提供するためのデータを保持するファイルを新たに追加したり、また、データのアクセスに必要なキーを変更したりするための、いわゆる発券作業は、一般に、ユーザに発行し、市場に出回っているICカードを、そのICカードの管理者や製造メーカーなどが回収し、セキュリティ管理の整備された施設等で行われる。

#### 【0007】

即ち、一般に、ICカードは、例えば、図31に示すように、ICカードの発行者が、1次発行作業を行い、ファンクションのないICカード（データの読み書きのできない状態のICカード）を、発券作業を行う発券業者に発行する。発券業者は、そのICカードによってサービスを提供しようとする管理者#1がICカードを利用できるように発券作業（2次発行作業）を行う。即ち、発券業者は、ICカードの中に、管理者#1が利用する記憶領域（管理者#1の領域）を確保し、さらに、管理者#1が、その記憶領域にアクセスするのに必要なキーその他の情報を書き込む。ここで、発券作業は、例えば、発券業者の施設などの、セキュリティ管理の整備された場所（以下、適宜、安全な場所という）で行われる。また、図31において、発券業者および管理者#1は、同一人である場合が多い。

【0008】

発券作業の行われたICカードは、市場に出荷され、ユーザに配布等される。そして、管理者#1がサービスを提供するのに利用される。即ち、これにより、ユーザは、ICカードを、例えば、電子的な定期券や財布として利用することができる。

【0009】

以上のようにして市場に出回ったICカードが、例えば、マルチファンクションのものであり、管理者#1以外の管理者#2が、そのマルチファンクションのICカードによってサービスの提供を行おうとする場合には、発券業者は、図3-2に示すように、市場に出回っているICカードを、一旦回収する。そして、発券業者は、管理者#2がICカードを利用することができるように発券作業を行う。即ち、ICカードの中に、管理者#2が利用する記憶領域（管理者#2の領域）を確保し、さらに、管理者#2が、その記憶領域にアクセスするのに必要なキーその他の情報を書き込む。その後、発券作業の行われたICカードは、再び、市場に出荷される。

【0010】

発券作業によってICカードに書き込まれる、例えば、キーなどは、ICカードのセキュリティ上重要な情報であり、このような情報を、市場などの、盗聴や改竄等の不正行為が行われる蓋然性の高い、セキュリティ管理のなされていない場所（以下、適宜、安全でない場所という）に流通させることは好ましくない。このため、発券作業は、上述のように、ICカードを、市場から回収し、安全な場所で行われる。

【0011】

従って、発券作業を行うごとに、ICカードを回収しなければならず、面倒であった。

【0012】

本発明は、このような状況に鑑みてなされたものであり、記憶領域にアクセスするのに必要なキーその他の情報を、セキュリティ上安全でない場所においても、安全に書き込むことができるようにするものである。

【0013】

【課題を解決するための手段】

請求項1に記載の情報処理装置は、データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報を暗号化する暗号化手段を備えることを特徴とする。

【0014】

請求項5に記載の情報処理方法は、データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報を暗号化する暗号化ステップを備えることを特徴とする。

【0015】

請求項6に記載の情報処理装置は、データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報であって、暗号化されたものを復号する復号手段を備えることを特徴とする。

【0016】

請求項10に記載の情報処理方法は、データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報であって、暗号化されたものを復号する復号ステップを備えることを特徴とする。

【0017】

請求項1に記載の情報処理装置においては、暗号化手段が、データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報を暗号化するようになされている。

【0018】

請求項5に記載の情報処理方法においては、データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報を暗号化するようになされている。

【0019】

請求項6に記載の情報処理装置においては、復号手段が、データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報であって、暗号化されたものを復号するようになされている。

【0020】

請求項10に記載の情報処理方法においては、データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報をあって、暗号化されたものを復号するようになされている。

【0021】

【発明の実施の形態】

以下に、本発明の実施の形態を説明するが、その前に、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し、一例）を付加して、本発明の特徴を記述すると、次のようになる。

【0022】

即ち、請求項1に記載の情報処理装置は、データを記憶するデータ記憶手段（例えば、図3に示すEEPROM66など）と、データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報を記憶する管理情報記憶手段（例えば、図3に示すEEPROM66など）と、管理情報に基づいて、データ記憶手段を管理する管理手段（例えば、図3に示すシーケンサ91など）とを備えるデータ記憶装置に対して、管理情報を提供するための処理を行う情報処理装置であって、管理情報を作成する作成手段（例えば、図28に示すプログラムの処理ステップS21など）と、管理情報を暗号化する暗号化手段（例えば、図28に示すプログラムの処理ステップS23など）とを備えることを特徴とする。

【0023】

請求項2に記載の情報処理装置は、管理情報が改竄されたか否かをチェックするためのチェックコードを演算する演算手段（例えば、図28に示すプログラムの処理ステップS22など）をさらに備え、暗号化手段が、管理情報とともに、チェックコードも暗号化することを特徴とする。

【0024】

請求項3に記載の情報処理装置は、暗号化された管理情報を、所定の伝送媒体を介して、データ記憶装置に送信する送信手段（例えば、図28に示すプログラ

ムの処理ステップS24など)をさらに備えることを特徴とする。

#### 【0025】

請求項6に記載の情報処理装置は、データを記憶するデータ記憶手段(例えば、図3に示すEEPROM66など)と、データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報を記憶する管理情報記憶手段(例えば、図3に示すEEPROM66など)と、管理情報に基づいて、データ記憶手段を管理する管理手段(例えば、図3に示すシーケンサ91など)とを備える情報処理装置であって、暗号化された管理情報を受信する受信手段(例えば、図3に示すインターフェイス部61など)と、暗号化された管理情報を復号する復号手段(例えば、図30に示すプログラムの処理ステップS32など)と、管理情報を、管理情報記憶手段に記憶させる記憶制御手段(例えば、図7に示すプログラムの処理ステップS4や、図8に示すプログラムの処理ステップS14など)とを備えることを特徴とする。

#### 【0026】

請求項7に記載の情報処理装置は、管理情報が改竄されたか否かをチェックするチェック手段(例えば、図30に示すプログラムの処理ステップS33など)をさらに備えることを特徴とする。

#### 【0027】

なお、勿論この記載は、各手段を上記したものに限定することを意味するものではない。

#### 【0028】

図1は、本発明を適用したICカードを用いた非接触カードシステム(システムとは、複数の装置が論理的に集合した物をいい、各構成の装置が同一筐体中にあるか否かは問わない)の一実施の形態の構成例を示している。

#### 【0029】

この非接触カードシステムは、R/W1、ICカード2、およびコントローラ3で構成され、R/W1とICカード2との間では、電磁波を利用して非接触で、データの送受信が行われるようになされている。

【0030】

即ち、R/W1が、所定のコマンドをICカード2に送信し、ICカード2は、そのコマンドを受信し、そのコマンドに対応する処理を行う。そして、ICカード2は、その処理結果に対応する応答データをR/W1に送信する。

【0031】

R/W1は、所定のインターフェース（例えば、RS-485Aの規格などに準拠したもの）を介してコントローラ3に接続されており、コントローラ3は、R/W1に対して所定の制御信号を供給することで、所定の処理を行わせる。

【0032】

図2は、図1のR/W1の構成例を示している。

【0033】

IC21においては、データの処理を行うDPU (Data Processing Unit) 31、ICカード2に送信するデータおよびICカード2から受信したデータの処理を行うSPU (Signal Processing Unit) 32、コントローラ3との通信を行うSCC (Serial Communication Controller) 33、およびデータの処理に必要な情報を予め記憶しているROM部41と処理途中のデータを一時的に記憶するRAM部42とで構成されるメモリ部34が、バスを介して接続されている。

【0034】

また、このバスには、所定のデータを記憶するフラッシュメモリ22も接続されている。

【0035】

DPU31は、ICカード2に送信するコマンドをSPU32に出力するとともに、ICカード2から受信した応答データをSPU32から受け取るようになされている。

【0036】

SPU32は、ICカード2に送信するコマンドに対して所定の処理（例えば、BPSK (BiPhase Shift Keying) 変調（ワンチェスタコードへのコーディング）など）を行った後、変調回路23に出力するとともに、ICカード2により送信されてきた応答データを復調回路25から受け取り、そのデータに対して所

定の処理を施すようになされている。

#### 【0037】

変調回路23は、発振器(OSC)26より供給される所定の周波数(例えば13.56MHz)の搬送波を、SPU32より供給されるデータで、ASK(Amplitude Shift Keying)変調し、生成された変調波をアンテナ27を介して、電磁波としてICカード2に出力するようになされている。なお、このとき、変調回路23は、変調度を1未満にして、ASK変調を行うようになされており、これにより、データがローレベルのときにおいても、変調波の最大振幅がゼロにならないようになされている。

#### 【0038】

復調回路25は、アンテナ27を介して受信した変調波(ASK変調波)を復調し、復調されたデータをSPU32に出力するようになされている。

#### 【0039】

図3は、図1のICカード2の構成例を示している。

#### 【0040】

このICカード2においては、IC51が、アンテナ53を介して、R/W1により送信された変調波を受信するようになされている。なお、コンデンサ52は、アンテナ53とともにLC回路を構成し、所定の周波数(キャリア周波数)の電磁波に同調(共振)するようになされている。

#### 【0041】

IC51において、RFインターフェース部61は、ASK復調部81で、アンテナ53を介して受信した変調波(ASK変調波)を検波して復調し、復調後のデータを、BPSK復調回路62およびPLL(Phase Locked Loop)部63に出力するとともに、電圧レギュレータ82で、ASK復調部81が検波した信号を安定化し、各回路に直流電源として供給するようになされている。

#### 【0042】

また、RFインターフェース部61は、発振回路83でデータのクロック周波数と同一の周波数の信号を発振し、その信号をPLL部63に出力するようになされている。

## 【0043】

さらに、RFインターフェース部61では、ASK変調部81において、演算部64より、BPSK変調回路68を介して供給されるデータに対応して、ICカード2の電源としてのアンテナ53の負荷を変動させる（例えば、データに対応して所定のスイッチング素子をオン／オフさせ、スイッチング素子がオン状態であるときだけ所定の負荷をアンテナ53に並列に接続させる）ことにより、アンテナ53を介して受信している変調波をASK変調し（ICカード2からデータを送信するときは（ICカード2にデータを送信させるときは）、R/W1は、その出力する変調波の最大振幅を一定にしており、この変調波が、アンテナ53の負荷の変動により、ASK変調される）、その変調成分を、アンテナ53を介してR/W1に送信する（R/W1のアンテナ27の端子電圧を変動させる）ようになされている。

## 【0044】

PLL部63は、ASK復調部81より供給されるデータから、そのデータに同期したクロック信号を生成し、そのクロック信号をBPSK復調回路62およびBPSK変調回路68に出力するようになされている。

## 【0045】

BPSK復調回路62は、ASK復調部81で復調されたデータが、BPSK変調されている場合、PLL部63より供給されたクロック信号に従って、そのデータの復調（ワンチェスタコードのデコード）を行い、復調したデータを演算部64に出力するようになされている。

## 【0046】

演算部64は、BPSK復調回路62より供給されたデータが暗号化されている場合、そのデータを暗号／復号部92で復号化した後、そのデータを、シーケンサ91で処理するようになされている。なお、データが暗号化されていない場合、BPSK復調回路62より供給されたデータは、暗号／復号部92を介さず、シーケンサ91に、直接供給される。

## 【0047】

シーケンサ91は、そこに供給されるコマンドとしてのデータに対応する処理

を行うようになされている。即ち、例えば、シーケンサ91は、EEPROM66に対するデータの書き込みや読み出し、その他データに対する必要な演算処理などを行う。さらに、シーケンサ91は、認証を行うことによるEEPROM66へのアクセス制御や、EEPROM66の管理などをも行うようになされている。

## 【0048】

演算部64のパリティ演算部93は、EEPROM66に記憶されるデータや、EEPROM66に記憶されているデータから、パリティとして、例えば、リードソロモン符号を算出するようになされている。

## 【0049】

さらに、演算部64は、シーケンサ91で所定の処理を行った後、その処理に対応する応答データ（R/W1に送信するデータ）をBPSK変調回路68に出力するようになされている。

## 【0050】

BPSK変調回路68は、演算部64より供給されたデータをBPSK変調し、変調後のデータをRFインターフェース部61のASK変調部84に出力するようになされている。

## 【0051】

ROM (Read Only Memory) 65は、シーケンサ91が処理を行うためのプログラムその他の必要なデータを記憶している。RAM67は、シーケンサ91が処理を行うとき、その処理の途中のデータなどを、一時的に記憶するようになされている。

## 【0052】

EEPROM (Electrically Erasable and Programmable ROM) 66は、不揮発性のメモリであり、ICカード2がR/W1との通信を終了し、電力供給が停止した後も、データを記憶し続けるようになされている。

## 【0053】

次に、R/W1とICカード2との間のデータの送受信処理について説明する。

## 【0054】

R/W1(図2)は、アンテナ27から所定の電磁波を放射して、アンテナ27の負荷状態を監視し、ICカード2が接近することによる負荷状態の変化が検出されるまで待機する。なお、R/W1には、所定の短いパターンのデータでASK変調した電磁波を放射して、ICカード2への呼びかけを、ICカード2からの応答が一定時間内に得られるまで繰り返す処理(ポーリング)を行わせるようにしてよい。

## 【0055】

R/W1において、ICカード2の接近が検出されると、R/W1のSPU32は、所定の周波数(例えば、データのクロック周波数の2倍の周波数)の矩形波を搬送波として、ICカード2に送信するデータ(ICカード2に実行させる処理に対応するコマンドや、ICカード2に書き込むデータなど)で、BPSK変調を行い、生成した変調波(BPSK変調信号)(ワンチェスタコード)を変調回路23に出力する。

## 【0056】

なお、BPSK変調時においては、差動変換を利用して、変調波の位相の変化に、データを対応させることができ、このようにした場合、BPSK変調信号が反転しても、元のデータに復調されるので、復調するとき変調波の極性を配慮する必要が無くなる。

## 【0057】

変調回路23は、入力されたBPSK変調信号で、所定の搬送波を1未満(例えば0.1)の変調度(=データ信号の最大振幅/搬送波の最大振幅)でASK変調し、生成された変調波(ASK変調波)を、アンテナ27を介してICカード2に送信する。

## 【0058】

なお、送信を行わないとき、変調回路23は、ディジタル信号の2つのレベル(ハイレベルとローレベル)のうちの、例えばハイレベルで変調波を生成するようになされている。

## 【0059】

ICカード2(図3)では、アンテナ53およびコンデンサ52で構成されるLC回路において、R/W1のアンテナ27が放射した電磁波の一部が電気信号に変換され、その電気信号(変調波)が、IC51のRFインターフェース61に出力される。そして、RFインターフェース61のASK復調部81は、その変調波を整流平滑化することで、包絡線検波を行い、これにより生成される信号を電圧レギュレータ82に供給するとともに、その信号の直流成分を抑制してデータ信号を抽出し、そのデータ信号をBPSK復調回路62およびPLL部63に出力する。

## 【0060】

なお、このとき、アンテナ53の端子電圧 $V_0$ は、例えば次のようになる。

$$V_0 = V_{10} (1 + k \times V_s(t)) \cos(\omega t)$$

但し、 $V_{10} \cos(\omega t)$ は、搬送波を、kは変調度を、 $V_s(t)$ はSPU32が出力するデータを、それぞれ表す。

## 【0061】

また、ASK復調部81による整流後の電圧 $V_1$ におけるローレベルの値 $V_{LR}$ は、例えば次のようになる。

$$V_{LR} = V_{10} (1 + k \times (-1)) - V_f$$

## 【0062】

ここで、 $V_f$ は、ASK復調部81において、整流平滑化を行うための整流回路を構成するダイオード(図示せず)における電圧降下を示しており、一般に0.7ボルト程度である。

## 【0063】

電圧レギュレータ82は、ASK復調部81により整流平滑化された信号を受信すると、その信号を安定化し、直流電源として、演算部64を始めとする各回路に供給する。なお、ここでは、上述したように、変調波の変調度kは1未満であるので、整流後の電圧変動(ハイレベルとローレベルの差)が小さい。従って、電圧レギュレータ82において、直流電源を容易に生成することができる。

## 【0064】

ここで、例えば、変調度  $k$  が 5 % の変調波を、  $V_{10}$  が 3 ボルト以上になるよう受信した場合、整流後のローレベル電圧  $V_{LR}$  は、  $2.15 (= 3 \times (1 - 0.05) - 0.7)$  ボルト以上となり、電圧レギュレータ 82 は、電源として充分な電圧を各回路に供給することができる。さらに、この場合、整流後の電圧  $V_1$  の交流成分（データ成分）の振幅  $2 \times k \times V_{10}$  (Peak-to-Peak 値) は、  $0.3 (= 2 \times 0.05 \times 3)$  ボルト以上になり、ASK 変調部 81 は、十分高い S/N 比でデータの復調を行うことができる。

## 【0065】

このように、変調度  $k$  が 1 未満の ASK 変調波を利用することにより、エラーレートの低い (S/N 比の高い状態で) 通信を行うとともに、電源として充分な直流電圧が IC カード 2 に供給される。

## 【0066】

BPSK 変調回路 62 は、ASK 変調部 81 からデータ信号 (BPSK 変調信号) を受信すると、そのデータ信号を、PLL 部 63 より供給されるクロック信号に従って復調し、復調したデータを演算部 64 に出力する。

## 【0067】

演算部 64 は、BPSK 変調回路 62 より供給されたデータが暗号化されている場合は、暗号/復号部 92 で復号化した後、そのデータ (コマンド) をシーケンサ 91 に供給して処理する。なお、この期間、即ち、IC カード 2 にデータを送信後、それに対する返答を受信するまでの間、R/W1 は、値が 1 のデータを送信したまま待機している。従って、この期間においては、IC カード 2 は、最大振幅が一定である変調波を受信している。

## 【0068】

シーケンサ 91 は、処理が終了すると、その処理結果などについてのデータ (R/W1 に送信するデータ) を、BPSK 変調回路 68 に出力する。BPSK 変調回路 68 は、R/W1 の SPU32 と同様に、そのデータを BPSK 変調 (ワンチエスタコードにコーディング) した後、RF インタフェース部 61 の ASK 変調部 84 に出力する。

## 【0069】

そして、ASK変調部84は、アンテナ53の両端に接続される負荷を、スイッチング素子などを利用し、BPSK変調回路68からのデータに応じて変動させることにより、受信している変調波（ICカード2によるデータの送信時においては、上述したように、R/W1が出力する変調波の最大振幅は一定になっている）を、送信するデータに応じてASK変調し、これによりR/W1のアンテナ27の端子電圧を変動させて、そのデータをR/W1に送信する。

## 【0070】

一方、R/W1の変調回路23は、ICカード2からのデータの受信時においては、値が1（ハイレベル）のデータの送信を継続している。そして、復調回路25において、ICカード2のアンテナ53と電磁気的に結合しているアンテナ27の端子電圧の微小な変動（例えば、数十マイクロボルト）から、ICカード2により送信されてきたデータが検出される。

## 【0071】

さらに、復調回路25では、検出した信号（ASK変調波）が高利得の増幅器（図示せず）で増幅されて復調され、その結果得られるデジタルデータがSPU32に出力される。SPU32は、そのデータ（BPSK変調信号）を復調し、DPU31に出力する。DPU31は、SPU32からのデータを処理し、その処理結果に応じて、通信を終了するか否かを判断する。そして、再度、通信を行うと判断した場合、上述した場合と同様にして、R/W1とICカード2との間で通信が行われる。一方、通信を終了すると判断した場合、R/W1は、ICカード2との通信処理を終了する。

## 【0072】

以上のように、R/W1は、変調度kが1未満であるASK変調を利用して、ICカード2にデータを送信し、ICカード2は、そのデータを受け取り、そのデータに対応する処理を行って、その処理の結果に対応するデータを、R/W1に返送する。

## 【0073】

次に、図4は、図3のEEPROM66の論理フォーマットを示している。

## 【0074】

E E P R O M 6 6 は、ブロックを単位として構成され、図4の実施の形態では、1ブロックは、例えば、16バイトで構成されている。

## 【0075】

さらに、図4の実施の形態では、最も上のブロックの論理アドレスを#0000h（hは、16進数を表す）として、昇順に、論理アドレスが付されている。なお、図4では、論理アドレスとして、#0000h乃至#FFFFhが付されており、従って、65536（=2<sup>16</sup>）個のブロックが構成されている。

## 【0076】

ブロックは、ユーザブロックまたはシステムブロックとして使用されるようになされている。E E P R O M 6 6 のブロックは、論理アドレスの昇順に、ユーザブロックに割り当てられていき、また、論理アドレスの降順に、システムブロックに割り当てられていくようになされている。即ち、図4において、ユーザブロックは下方向に、システムブロックは上方向に、それぞれ増えていき、空きブロックがなくなった時点で、ユーザブロックおよびシステムブロックをつくることはできなくなる。従って、ユーザブロックとシステムブロックとの境界は固定ではなく、また、ユーザブロックの数、またはシステムブロックの数それぞれには、特に制限がない（但し、図4の実施の形態では、ユーザブロックとシステムブロックとの合計は、65536個以下に制限される）。

## 【0077】

システムブロックには、製造ID（Identification）ブロック、発行IDブロック、システム定義ブロック、エリア定義ブロック、サービス定義ブロックの5種類がある。なお、図4の実施の形態では、エリア定義ブロックまたはサービス定義ブロックとなっているブロックを、エリア／サービス定義ブロックと示してある。

## 【0078】

システムブロックのうち、製造IDブロック、発行IDブロック、システム定義ブロックの3つは、基本的に、I Cカード2の発行時には、既に配置されているもので、論理アドレス#FFFFh, #FFFEh, #FFF Dhにそれぞれ

配置される。そして、エリア／サービス定義ブロックは、論理アドレス #FFFCh より上に、作成順に配置されていく。

#### 【0079】

製造 ID ブロックには、IC カード 2 の製造に関する情報が配置される。即ち、製造 ID ブロックには、例えば、ユニークな製造 ID や、製造年月日、製造者のコードなどが配置される。

#### 【0080】

発行 ID ブロックには、IC カード 2 の発行に関する情報が配置される。即ち、発行 ID ブロックには、例えば、IC カード 2 が発行された日付や、IC カードを発行した順番を表すコードなどが配置される。

#### 【0081】

システム定義ブロックには、例えば、EEPROM66 が有するシステムブロックまたはユーザブロックの数や、システムキーなどが配置される。なお、システムキーは、IC カード 2 と、R/W1 およびコントローラ 3との間で、相互認証を行うときに用いられる。

#### 【0082】

エリア定義ブロックは、例えば、EEPROM66 の記憶領域（エリア）が、管理者に割り当てられることにより作成され、そこには、管理者が、自身に割り当てられた記憶領域を管理するための情報などが配置される。即ち、エリア定義ブロックには、例えば、後述するコード範囲、空き容量、およびエリアキーなどが配置される。

#### 【0083】

サービス定義ブロックには、後述するサービス領域を管理するための情報（サービス領域の容量やサービスキーなど）などが配置される。

#### 【0084】

次に、シーケンサ 91 では、EEPROM66 の記憶領域が階層化されて管理されるようになされている。

#### 【0085】

即ち、図 5 は、EEPROM66 のディレクトリ構造を示している。

【0086】

E E P R O M 6 6 の記憶領域は、エリア定義領域を階層とする階層構造をなしており、エリア定義領域は、エリア定義領域およびサービス定義領域を有することができるようになされている。

【0087】

エリア定義領域は、管理者に割り当てられ、そこには、管理者が、エリア定義領域やサービス定義領域を識別するための名前として使用可能な識別コードの範囲を表すコード範囲、使用可能な空きブロック数を表す空き容量、認証に用いる、後述するアクセスキーを生成するためのエリアキーなどが配置される。ここで、1のエリア定義領域は、図4で説明した1のエリア定義ブロックに対応する。

【0088】

図5の実施の形態では、管理者Aに割り当てられたエリア定義領域が最上位階層を構成しており、これを親の階層として、管理者B1およびB2のエリア定義領域が作成されている。さらに、管理者B1のエリア定義領域を、親の階層として、管理者Cのエリア定義領域が作成されている。

【0089】

サービス定義領域は、管理者が提供するサービスに割り当てられ、そこには、そのサービスの提供に必要なデータを記憶するサービス領域の容量や、アクセスキーを生成するためのサービスキーなどが配置される。ここで、1のサービス定義領域は、図4で説明した1のサービス定義ブロックに対応する。

【0090】

サービス領域は、サービスの提供に必要なデータが記憶される記憶領域で、図4のユーザブロックに対応する。即ち、サービス領域は、0以上のユーザブロックで構成され、サービス領域を構成するユーザブロック数が、そのサービス領域を管理するサービス定義領域の容量として配置される。

【0091】

また、エリア定義領域およびサービス定義領域には、それらを識別するための識別コードも配置される。ここで、エリア定義領域またはサービス定義領域を識別するための識別コードそれぞれを、以下、適宜、エリアコードまたはサービス

コードという。なお、サービスコードは、あるサービス領域を管理するサービス定義領域を識別するものであるから、そのサービス領域を識別する識別コード（サービス領域識別コード）であるということもできる。

#### 【0092】

図5の実施の形態では、管理者Aに、最上位階層のエリア定義領域が割り当てられている。そして、使用可能な識別コードの範囲（コード範囲）として、0000h乃至FFFhが、エリアキーとして、0123456789abcdefが、それぞれ定義されている。ここで、エリア定義領域におけるコード範囲内の識別コードであれば、いずれの識別コードも、そのエリア定義領域のエリアコードとして使用可能であるが、本実施の形態では、例えば、エリア定義領域のコード範囲の最小値が、そのエリアコードとして使用されるようになされている。従って、コード範囲が、0000h乃至FFFhとなっているエリア定義領域、即ち、管理者Aに割り当てられているエリア定義領域のエリアコードは、0000hとなっている。ここで、エリアコード#xxxxxhのエリア定義領域を、以下、適宜、エリア定義領域#xxxxxhと記載する。

#### 【0093】

管理者Aのエリア定義領域#0000hの階層には、管理者Aがサービスを提供するためのサービス定義領域が設けられている。このサービス定義領域には、エリア定義領域#0000hのコード範囲である0000h乃至FFFhのうち、0008hが、サービスコードとして割り当てられている。ここで、サービスコード#xxxxxhのサービス定義領域を、以下、適宜、サービス定義領域#xxxxxhと記載する。

#### 【0094】

サービス定義領域#0008hの容量は8とされており、従って、8のユーザブロックで構成されるサービス領域の使用が可能となっている。また、サービス定義領域#0008hのサービスキーは、0101010101010101となっている。

#### 【0095】

さらに、管理者Aのエリア定義領域#0000hの階層には、管理者B1のエリア定義領域#0100h、および管理者B2のエリア定義領域#1000hが

、その子の階層として設けられている。また、エリア定義領域#0000hの階層には、図示せぬその他のエリア定義領域も設けられており、これにより、エリア定義領域#0000hが使用可能なブロック数（空き容量）は、例えば、37ブロックとなっている。

[0096]

管理者B1のエリア定義領域#0100hのコード範囲としては、その親の階層であるエリア定義領域#0000hのコード範囲である0000h乃至FFFhのうちの、0100h乃至03FFhが割り当てられている。ここで、管理者B1のエリア定義領域のコード範囲が0100h乃至03FFhであるため、その最小値である0100hが、管理者B1のエリア定義領域のエリヤコードとなっている。

[0097]

[0098]

さらに、管理者Bのエリア定義領域#0100hの階層には、管理者Cのエリア定義領域#0300hが、その子の階層として設けられている。そして、管理者Cのエリア定義領域#0300hのコード範囲としては、その親の階層であるエリア定義領域#0100hのコード範囲である0100h乃至03FFhのうちの、0300h乃至03FFhが割り当てられている。ここで、管理者Cのエリア定義領域のコード範囲が0300h乃至03FFhであるため、その最小値である0300hが、管理者Cのエリア定義領域のエリヤコードとなっている。

[0099]

[0 1 0 0]

管理者Cのエリア定義領域#0300hの階層には、管理者Cがサービスを提供するためのサービス定義領域が設けられている。このサービス定義領域には、

エリア定義領域#0300hのコード範囲である0300h乃至03FFhのうちの、030Chが、サービスコードとして割り当てられている。

[0 1 0 1]

このサービスコード 030Ch が割り当てられているサービス定義領域、即ち、サービス定義領域 #030Ch の容量は 16 とされており、従って、16 のユーザブロックで構成されるサービス領域の使用が可能となっている。また、サービス定義領域 #030Ch のサービスキーは、02020202020202 となっている。

[0102]

ここで、サービス定義領域 #030Ch が管理するサービス領域の容量が 16 であり、そのサービス定義領域 #030Ch 自体が、1 のブロックを、サービス定義ブロックとして使用することから、サービス定義領域 #030Ch が存在することによって使用されるブロック数は 17 (= 16 + 1) ブロックとなる。また、サービス定義領域 #030Ch が属する階層のエリア定義領域 #0300h が使用可能なブロック数は、その空き容量が 0 であるから、0 ブロックである。さらに、エリア定義領域 #0300h 自体が、1 のブロックを、エリア定義ブロックとして使用する。従って、エリア定義領域 #0300h の階層においては、使用されているブロックが 18 (= 17 + 1) ブロックで、使用可能なブロックが 0 ブロックであるから、その親の階層（上位階層）であるエリア定義領域 #0100h から割り当てられたブロック数が、18 (= 18 + 0) ブロックであることが分かる。

[0 1 0 3]

さらに、エリア定義領域 # 0100 h の階層については、その子の階層（下位階層）であるエリア定義領域 # 0300 h で、上述のように、18 ブロックが使用されている。また、エリア定義領域 # 0100 h 自体が 1 のブロックを、エリア定義ブロックとして使用している。そして、エリア定義領域 # 0100 h の空き容量は、上述したように 14 となっている。従って、エリア定義領域 # 0100 h の階層においては、使用されているブロックが 19 (= 18 + 1) ブロックで、使用可能なブロックが 14 であるから、その親の階層であるエリア定義領域 # 0000 h から割り当てられたブロックは、33 (= 19 + 14) ブロックで

あることが分かる。

[0104]

一方、管理者B2のエリア定義領域#1000hのコード範囲としては、その親の階層であるエリア定義領域#0000hのコード範囲である0000h乃至FFFhのうちの、1000h乃至1FFFhが割り当てられている。ここで、管理者B2のエリア定義領域のコード範囲が1000h乃至1FFFhであるため、その最小値である1000hが、管理者B2のエリア定義領域のエリヤコードとなっている。

[0105]

また、エリア定義領域 # 1000 h の空き容量またはエリアキーは、それぞれ  
、43 または c0c0c0c0c0c0c0c0c0c0 になっている。

[0106]

管理者 B 2 のエリア定義領域 # 1 0 0 0 h の階層には、管理者 B 2 がサービスを提供するためのサービス定義領域が設けられている。このサービス定義領域には、エリア定義領域 # 1 0 0 0 h のコード範囲である 1 0 0 0 h 乃至 1 F F F h のうちの、1 0 2 2 h が、サービスコードとして割り当てられている。

【0107】

このサービスコード1022hが割り当てられているサービス定義領域、即ち、サービス定義領域#1022hの容量は4とされており、従って、4のユーザブロックで構成されるサービス領域の使用が可能となっている。また、サービス定義領域#1022hのサービスキーは、0303030303030303となっている。

[0108]

ここで、サービス定義領域 # 1022h が管理するサービス領域の容量が 4 であり、そのサービス定義領域 # 1022h 自体が、1 のブロックを、サービス定義ブロックとして使用することから、サービス定義領域 # 1022h が存在することによって使用されるブロック数は  $5 (= 4 + 1)$  ブロックとなる。また、サービス定義領域 # 1022h が属する階層のエリア定義領域 # 1000h が使用可能なブロック数は、その空き容量が 43 であるから、43 ブロックである。さらに、エリア定義領域 # 1000h 自体が 1 のブロックを、エリア定義ブロック

として使用している。従って、エリア定義領域 #1000 h の階層においては、使用されているブロックが 6 (= 5 + 1) ブロックで、使用可能なブロックが 43 ブロックであるから、エリア定義領域 #1000 h に割り当てられたブロックは、49 (= 6 + 43) ブロックであることが分かる。

#### 【0109】

以上のように、管理対象のエリア定義領域に割り当て可能な識別コードの範囲であるコード範囲をエリア定義領域に記憶させるようにしたので、そのコード範囲に基づき、管理対象のエリア定義領域を子の階層とし、そのエリア定義領域を管理するエリア定義領域を親の階層とする、図 5 に示したような階層構造を規定することができる。

#### 【0110】

次に、図 6 を参照して、最上位階層のエリア定義領域 #0000 h が割り当てられた管理者 A が、例えば、IC カード 2 の発行者であるとして、図 5 に示した階層構造が構成されていく過程について説明する。

#### 【0111】

管理者 A は、例えば、ユーザの要求に応じて、IC カード 2 を発行する (1)。この IC カード 2 には、図 5 の階層構造のうち、例えば、エリア定義領域 #0000 h だけが作成されている。

#### 【0112】

そして、管理者 A は、サービス定義領域 #0008 h によって管理されるサービス領域を利用して、所定のサービスの提供を開始する場合、そのサービス定義領域 #0008 h の作成を行うのに必要な情報を、発券機 101 に登録する (2)。

#### 【0113】

ここで、発券機 101 は、例えば、図 1 の R/W1 とコントローラ 3 から構成される。また、発券機 101 は、例えば、駅や、小売店、その他の施設などに設置することができる。

#### 【0114】

その後、ユーザが、IC カード 2 を、発券機 101 に装着すると (IC カード

2を、発券機101が内蔵するR/W1との間で通信を行うことが可能な状態にすると）、発券機101は、発券作業を行い、即ち、登録された情報に基づいて、ICカード2にコマンドおよび必要なデータを送信し、サービス定義領域#0008hを作成させる。これにより、ユーザは、サービス定義領域#0008hによって管理されるサービス領域を利用した、管理者Aによるサービスの提供を受けることが可能となる。

#### 【0115】

一方、管理者B1、B2それぞれは、ICカード2を利用したサービスの提供を行いたい場合、管理者Aとの間で契約を結び、管理者Aに、エリア定義領域#0100hおよび#1000hの作成を行うのに必要な情報を、発券機101に登録してもらう（3）、（4）。そして、ユーザが、ICカード2を、発券機101に装着すると、発券機101は、発券作業を行い、即ち、登録された情報に基づいて、ICカード2にコマンドおよび必要なデータを送信し、エリア定義領域#0100hおよび#1000hを作成させる。これにより、管理者B1またはB2は、エリア定義領域#0100hまたは#1000hにおいて定義されている範囲内において、ICカード2のリソースを使用することが可能となる。なお、この場合、管理者B1、B2に対する発券業者は、管理者Aということになる。

#### 【0116】

その後、管理者B2が、サービス定義領域#1022hによって管理されるサービス領域を利用して、所定のサービスの提供を開始する場合、そのサービス定義領域#1022hの作成を行うのに必要な情報を、発券機101に登録する（5）。そして、ユーザが、ICカード2を、発券機101に装着すると、発券機101は、登録された情報に基づいて、ICカード2にコマンドおよび必要なデータを送信し、サービス定義領域#1022hを作成させる。これにより、ユーザは、サービス定義領域#1022hによって管理されるサービス領域を利用した、管理者B2によるサービスの提供を受けることが可能となる。

#### 【0117】

また、管理者Cは、管理者B1の管理下において、ICカード2を利用したサ

ービスの提供を行いたい場合、管理者B1との間で契約を結び、管理者B1に、エリア定義領域#0300hの作成を行うのに必要な情報を、発券機101に登録してもらう（6）。そして、ユーザが、ICカード2を、発券機101に装着すると、発券機101は、登録された情報に基づいて、ICカード2にコマンドおよび必要なデータを送信し、エリア定義領域#0300hを作成させる。これにより、管理者Cは、エリア定義領域#0300hにおいて定義されている範囲内において、ICカード2のリソースを使用することが可能となる。なお、この場合、管理者Cに対する発券業者は、管理者B1ということになる。

#### 【0118】

その後、管理者Cが、サービス定義領域#030Chによって管理されるサービス領域を利用して、所定のサービスの提供を開始する場合、そのサービス定義領域#030Chの作成を行うのに必要な情報を、発券機101に登録する（7）。そして、ユーザが、ICカード2を、発券機101に装着すると、発券機101は、登録された情報に基づいて、ICカード2にコマンドおよび必要なデータを送信し、サービス定義領域#030Chを作成させる。これにより、ユーザは、サービス定義領域#030Chによって管理されるサービス領域を利用した、管理者Cによるサービスの提供を受けることが可能となる。

#### 【0119】

ICカード2では、以上のように、発券機101からのコマンドにしたがって、エリア定義領域やサービス定義領域が作成される。このエリア定義領域を作成するエリア作成処理、およびサービス定義領域を作成するサービス作成処理は、例えば、シーケンサ91によって行われるが、このエリア作成処理およびサービス作成処理について、図7および図8を参照して説明する。

#### 【0120】

まず最初に、図7のフローチャートを参照して、エリア作成処理について説明する。

#### 【0121】

ICカード2が発券機101に装着されると、発券機101は、例えば、ICカード2に対して、エリア定義領域を作成することを指令するコマンド（以下、

定義、エリア作成コマンドという)と、そのエリア定義領域を作成するために必要な情報、即ち、例えば、作成するエリア定義領域のコード範囲、そのエリア定義領域に割り当てられたブロック数(以下、適宜、割り当てブロック数という)、およびエリアキーなどを送信する。

#### 【0122】

ICカード2(シーケンサ91)は、エリア作成コマンドを受信すると、それとともに送信されてくる作成対象のエリア定義領域のコード範囲、割り当てブロック数、およびエリアキーなどを認識する。さらに、ICカード2では、作成対象のエリア定義領域のエリアコードを認識する。即ち、ここでは、作成対象のエリア定義領域のコード範囲の最小値が、そのエリアコードとして認識される。また、ICカード2では、作成対象のエリア定義領域のコード範囲を含むコード範囲を有するエリア定義領域が、作成対象のエリア定義領域の親の階層のエリア定義領域として認識される。

#### 【0123】

そして、ICカード2では、ステップS1において、作成対象のエリア定義領域が、EEPROM66の中に既に作成されているかどうかが判定される。即ち、ステップS1では、作成対象のエリア定義領域のエリアコードと同一のエリアコードを有するエリア定義領域が、既に作成されているかどうかが判定される。

#### 【0124】

ステップS1において、作成対象のエリア定義領域が既に作成されていると判定された場合、エリア作成処理を終了する。即ち、作成対象のエリア定義領域が既に作成されている場合は、同一のエリア定義領域を重複して作成する必要はないから、以降の処理は行われない。

#### 【0125】

また、ステップS1において、作成対象のエリア定義領域が作成されていないと判定された場合、ステップS2に進み、作成対象のエリア定義領域のコード範囲および割り当てブロック数(容量)が適正かどうかが判定される。即ち、ステップS2では、作成対象のエリア定義領域のコード範囲が、親の階層のエリア定義領域に記憶されているコード範囲に含まれており、かつ作成対象のエリア定義

領域の割り当てブロック数が、親の階層のエリア定義領域に記憶されている空き容量以下であるかどうかが判定される。

#### 【0126】

ステップS2において、作成対象のエリア定義領域のコード範囲および割り当てブロック数が適正でないと判定された場合、即ち、作成対象のエリア定義領域のコード範囲が、親の階層のエリア定義領域に記憶されているコード範囲に含まれていないか、または作成対象のエリア定義領域の割り当てブロック数が、親の階層のエリア定義領域に記憶されている空き容量を越えている場合、ステップS3に進み、エラー処理が行われ、エリア作成処理を終了する。即ち、ステップS3では、例えば、親の階層のエリア定義領域の子の階層として、エリア定義領域を作成することができない旨のメッセージが、発券機101に送信される。従って、この場合、エリア定義領域は作成されない（発券作業は行われない）。

#### 【0127】

一方、ステップS2において、作成対象のエリア定義領域のコード範囲および割り当てブロック数が適正であると判定された場合、即ち、作成対象のエリア定義領域のコード範囲が、親の階層のエリア定義領域に記憶されているコード範囲に含まれおり、かつ作成対象のエリア定義領域の割り当てブロック数が、親の階層のエリア定義領域に記憶されている空き容量以下である場合、ステップS4に進み、作成対象のエリア定義領域が、親の階層のエリア定義領域の子の階層として作成される。

#### 【0128】

即ち、ステップS4では、EEPROM66（図4）の中の空きブロックのうち、最も下のブロック（論理アドレスの最も大きい空きブロック）が、作成対象のエリア定義領域に対応するエリア定義ブロックとして確保される。さらに、そのエリア定義ブロックに、コード範囲、空き容量、エリアキーなどが書き込まれる（記憶される）。ここで、ステップS4では、コード範囲およびエリアキーとしては、発券機101から送信されてきたものが、そのまま書き込まれる。また、空き容量としては、発券機101から送信されてきた割り当てブロック数から1を減算した値が書き込まれる。なお、空き容量として、割り当てブロック数か

ら1を減算した値を書き込むのは、作成されたエリア定義領域が、1のブロックを使用するためである。

#### 【0129】

その後、ステップS5に進み、親の階層のエリア定義領域の空き容量が書き換えられ、エリア作成処理を終了する。即ち、ステップS5では、親の階層のエリア定義領域の空き容量から、割り当てブロック数を減算した値が、その親の階層のエリア定義領域の空き容量として、新たに書き込まれる。

#### 【0130】

図5に示した管理者B1, B2, Cそれぞれのエリア定義領域#0100h, #1000h, #0300hは、以上のエリア作成処理が行われることで作成される。

#### 【0131】

即ち、ICカード2の発行時において、その発行者でもある管理者Aが、ICカード2のリソースすべてを有しており、ICカード2の使用可能な識別コードまたは容量が、例えば、0000h乃至FFFhまたは65533ブロックであるとすると、ICカード2の発行時においては、エリア定義領域としては、コード範囲が0000h乃至FFFhで、空き容量が65532となっている、最上位階層のエリア定義領域#0000hだけが存在している。

#### 【0132】

なお、本実施の形態では、図4に示したように、EEPROM66は、65536のブロックを有しているが、発行直後のICカード2において、使用可能な容量が、それより3ブロック少ない65533ブロックであるのは、図4に示したように、製造IDブロック、発行IDブロック、システム定義ブロックが存在するためである。

#### 【0133】

また、最上位階層のエリア定義領域#0000hの空き容量が、使用可能な容量である65533ブロックより1ブロック少ない65532ブロックとなるのは、エリア定義領域#0000h自体が、1ブロックを使用するためである。

【0134】

管理者Aが、自身のリソースのうち、例えば、0100h乃至03FFhの範囲の識別コードと、33ブロックを、管理者B1に分け与える場合には、エリア作成処理が行われることにより、エリア定義領域#0100hが作成される。即ち、この場合、0100h乃至03FFhがコード範囲として、また、32ブロックが空き容量として、エリア定義領域#0100hに書き込まれる。なお、空き容量が、管理者Aから分け与えられる33ブロックより1ブロック少ないのは、エリア定義領域#0100h自体が、1ブロックを使用するからである。

【0135】

エリア定義領域#0100hが作成されると、管理者Aのエリア定義領域#0000hの空き容量は、管理者B1に分け与えた33ブロックだけ減らされる。

【0136】

また、管理者Aが、自身のリソースのうち、例えば、1000h乃至1FFFhの範囲の識別コードと、49ブロックを、管理者B2に分け与える場合には、エリア作成処理が行われることにより、エリア定義領域#1000hが作成される。即ち、この場合、1000h乃至1FFFhがコード範囲として、また、48ブロックが空き容量として、エリア定義領域#1000hに書き込まれる。なお、空き容量が、管理者Aから分け与えられる49ブロックより1ブロック少ないのは、エリア定義領域#1000h自体が、1ブロックを使用するからである。

【0137】

エリア定義領域#1000hが作成されると、管理者Aのエリア定義領域#0000hの空き容量は、管理者B2に分け与えた33ブロックだけ減らされる。

【0138】

管理者B1またはB2それぞれは、以上のようにして、エリア定義領域#0100hまたは#1000hが作成されると、そのエリア定義領域#0100hまたは#1000hの階層に、その子の階層としてのエリア定義領域や、サービス定義領域を作成することが可能となる。

## 【0139】

例えば、いま、管理者B1が、自身のリソースのうち、例えば、0300h乃至03FFhの範囲の識別コードと、18ブロックを、管理者Cに分け与える場合には、エリア作成処理が行われることにより、エリア定義領域#0300hが作成される。即ち、この場合、0300h乃至03FFhがコード範囲として、また、17ブロックが空き容量として、エリア定義領域#0300hに書き込まれる。なお、空き容量が、管理者B1から分け与えられる18ブロックより1ブロック少ないので、エリア定義領域#0300h自体が、1ブロックを使用するからである。

## 【0140】

エリア定義領域#0300hが作成されると、管理者B1エリア定義領域#0100hの空き容量は、管理者Cに分け与えた18ブロックだけ減らされる。即ち、上述したように、エリア定義領域#0100hが作成された時点では、その空き領域は、32ブロックであったが、18ブロックだけ減らされて、図5に示したように、14ブロックとなる。

## 【0141】

次に、図8のフローチャートを参照して、サービス作成処理について説明する。

## 【0142】

ICカード2が発券機101に装着されると、発券機101は、ICカード2に対して、サービス定義領域を作成することを指令するコマンド（以下、定義、サービス作成コマンドという）と、そのサービス定義領域を作成するために必要な情報、即ち、例えば、作成するサービス定義領域のサービスコード、そのサービス定義領域に割り当てられたブロック数（これも、以下、適宜、割り当てブロック数という）、およびサービスキーなどを送信する。

## 【0143】

ICカード2（シーケンサ91）は、サービス作成コマンドを受信すると、それとともに送信されてくる作成対象のサービス定義領域のサービスコード、割り当てブロック数、およびサービスキーなどを認識する。さらに、ICカード2で

は、作成対象のサービス定義領域のサービスコードを含むコード範囲を有するエリア定義領域が、作成対象のサービス定義領域の親の階層のエリア定義領域として認識される。

#### 【0144】

そして、ICカード2では、ステップS11において、作成対象のサービス定義領域が、EEPROM66の中に既に作成されているかどうかが判定される。即ち、ステップS11では、作成対象のサービス定義領域のサービスコードと同一のサービスコードを有するサービス定義領域が、既に作成されているかどうかが判定される。

#### 【0145】

ステップS11において、作成対象のサービス定義領域が既に作成されていると判定された場合、サービス作成処理を終了する。即ち、作成対象のサービス定義領域が既に作成されている場合は、同一のサービス定義領域を重複して作成する必要はないから、以降の処理は行われない。

#### 【0146】

また、ステップS11において、作成対象のサービス定義領域が作成されていないと判定された場合、ステップS12に進み、作成対象のサービス定義領域のサービスコードおよび割り当てブロック数（容量）が適正かどうかが判定される。即ち、ステップS12では、作成対象のサービス定義領域のサービスコードが、親の階層のエリア定義領域に記憶されているコード範囲に含まれており、かつ作成対象のサービス定義領域の割り当てブロック数が、親の階層のエリア定義領域に記憶されている空き容量以下であるかどうかが判定される。

#### 【0147】

ステップS12において、作成対象のサービス定義領域のサービスコードおよび割り当てブロック数が適正でないと判定された場合、即ち、作成対象のサービス定義領域のサービスコードが、親の階層のエリア定義領域に記憶されているコード範囲に含まれていないか、または作成対象のサービス定義領域の割り当てブロック数が、親の階層のエリア定義領域に記憶されている空き容量を越えている場合、ステップS13に進み、エラー処理が行われ、エリア作成処理を終了する

。即ち、ステップS3では、例えば、親の階層のエリア定義領域の階層に、サービス定義領域を作成することができない旨のメッセージが、発券機101に送信される。従って、この場合、サービス定義領域は作成されない。

#### 【0148】

一方、ステップS12において、作成対象のサービス定義領域のサービスコードおよび割り当てブロック数が適正であると判定された場合、即ち、作成対象のサービス定義領域のサービスコードが、親の階層のエリア定義領域に記憶されているコード範囲に含まれおり、かつ作成対象のサービス定義領域の割り当てブロック数が、親の階層のエリア定義領域に記憶されている空き容量以下である場合、ステップS14に進み、作成対象のサービス定義領域が、親の階層のエリア定義領域の階層に作成される。

#### 【0149】

即ち、ステップS14では、EEPROM66(図4)の中の空きブロックのうち、最も下のブロック(論理アドレスの最も大きい空きブロック)が、作成対象のサービス定義領域に対応するサービス定義ブロックとして確保される。さらに、そのサービス定義ブロックに、サービスコード、容量、サービスキーなどが書き込まれる。ここで、ステップS14では、サービスコードおよびサービスキーとしては、発券機101から送信されてきたものが、そのまま書き込まれる。また、容量としては、発券機101から送信されてきた割り当てブロック数から1を減算した値が書き込まれる。なお、容量として、割り当てブロック数から1を減算した値を書き込むのは、作成されたサービス定義領域が、1のブロックを使用するためである。

#### 【0150】

また、ステップS14では、作成されたサービス定義領域に書き込まれた容量に対応する数の空きブロックが、論理アドレスの小さい順に選択され、そのサービス定義領域が管理するサービス領域を構成するユーザブロックとして確保され、ステップS15に進む。

#### 【0151】

ステップS15では、親の階層のエリア定義領域の空き容量が書き換えられ、

サービス作成処理を終了する。即ち、ステップS15では、親の階層のエリア定義領域の空き容量から、割り当てブロック数を減算した値が、そのエリア定義領域の空き容量として、新たに書き込まれる。

#### 【0152】

図5に示した管理者A, B2, Cそれぞれのサービス定義領域#0008h, #1022h, #030Chは、以上のサービス作成処理が行われることで作成される。

#### 【0153】

即ち、管理者Aが、自身のリソースのうち、例えば、0008hの識別コードと、9ブロックの容量を用いてサービスの提供を行う場合には、サービス作成処理が行われることにより、サービス定義領域#0008hが作成され、そこに、容量として、8ブロックが書き込まれる。さらに、8個の空きブロックがユーザブロックとして確保され、エリア定義領域#0008hによって管理されるサービス領域とされる。なお、サービス定義領域#0008hに書き込まれる容量が、9ブロックより1ブロック少ないのは、サービス定義領域#0008h自体が、1ブロックを使用するからである。

#### 【0154】

サービス定義領域#0008hが作成されると、管理者Aのエリア定義領域#0000hの空き容量は、サービス定義領域#0008hに分け与えた9ブロックだけ減らされる。

#### 【0155】

以上により、管理者Aは、サービス定義領域#0008hで管理される8ブロックのサービス領域を用いて、サービスを提供することが可能となる。

#### 【0156】

また、管理者B2が、自身のリソースのうち、例えば、1022hの識別コードと、5ブロックの容量を用いてサービスの提供を行う場合には、サービス作成処理が行われることにより、サービス定義領域#1022hが作成され、そこに、容量として、4ブロックが書き込まれる。さらに、4個の空きブロックがユーザブロックとして確保され、エリア定義領域#1022hによって管理されるサ

ービス領域とされる。なお、サービス定義領域#1022hに書き込まれる容量が、5ブロックより1ブロック少ないのは、サービス定義領域#1022h自体が、1ブロックを使用するからである。

#### 【0157】

サービス定義領域#1022hが作成されると、管理者B2のエリア定義領域#1000hの空き容量は、サービス定義領域#1022hに分け与えた5ブロックだけ減らされる。即ち、上述したように、エリア定義領域#1000hが作成された時点では、その空き容量は、48ブロックであったが、5ブロックだけ減らされて、図5に示したように、43ブロックとなる。

#### 【0158】

以上により、管理者B2は、サービス定義領域#1022hで管理される4ブロックのサービス領域を用いて、サービスを提供することが可能となる。

#### 【0159】

さらに、管理者Cが、自身のリソースのうち、例えば、030Chの識別コードと、17ブロックの容量を用いてサービスの提供を行う場合には、サービス作成処理が行われることにより、サービス定義領域#030Chが作成され、そこに、容量として、16ブロックが書き込まれる。さらに、16個の空きブロックがユーザブロックとして確保され、エリア定義領域#030Chによって管理されるサービス領域とされる。なお、サービス定義領域#030Chに書き込まれる容量が、17ブロックより1ブロック少ないのは、サービス定義領域#030Ch自体が、1ブロックを使用するからである。

#### 【0160】

サービス定義領域#030Chが作成されると、管理者Cのエリア定義領域#0300hの空き容量は、サービス定義領域#030Chに分け与えた17ブロックだけ減らされる。即ち、上述したように、エリア定義領域#0300hが作成された時点では、その空き容量は、17ブロックであったが、17ブロックだけ減らされて、図5に示したように、0ブロックとなる。

#### 【0161】

以上により、管理者Cは、サービス定義領域#030Chで管理される16ブ

ロックのサービス領域を用いて、サービスを提供することが可能となる。

#### 【0162】

以上のように、コード範囲および空き容量を記憶しているエリア定義領域に基づいて、EEPROM66を管理するようにしたので、ICカード2のリソース管理を行うことが可能となる。即ち、あるエリア定義領域の階層の中で使用可能な容量および識別コードを制限することができる。その結果、例えば、ある管理者が、自身に割り当てられたリソース（ここでは、使用可能な容量および識別コード）の一部を、他の管理者に分け与えて、ICカード2を共有したとしても、識別コードが、異なる管理者の間で重複することや、管理者が、あらかじめ、契約等で定められた容量を超えてEEPROM66を使用することなどを防止することができる。

#### 【0163】

次に、ICカード2では、図5で説明したように、EEPROM66の記憶領域が、エリア定義領域を階層とする階層構造をなしており、さらに、各エリア定義領域およびサービス定義領域に、認証のためのキー（本実施の形態では、エリア定義領域またはサービス定義領域のキーを、それぞれエリアキーまたはサービスキーと呼んでいる）が記憶されている結果、ICカード2に対するフレキシブルでセキュリティの高いアクセス制御を行うことが可能となっている。

#### 【0164】

即ち、管理者どうしの間において、例えば、図9に示すような情報のやりとりを行うことで、ICカード2に対するフレキシブルでセキュリティの高いアクセス制御を実現することができる。

#### 【0165】

具体的には、ICカード2の発行者でもある管理者Aは、EEPROM66（図4）のシステム定義ブロックに記憶させるシステムキーと、自身のエリア定義領域#0000hのエリアキーを決定し、システムキーをシステム定義ブロックに、エリアキー#0000hをエリア定義領域#0000hに、それぞれ記憶させておく。ここで、エリア定義領域#xxxxhのエリアキーを、以下、適宜、エリアキー#xxxxhと記載する。

【0166】

さらに、管理者Aは、システムキーを、エリアキー#0000hで暗号化し、エリア中間キー $K_A$ を生成しておく。なお、暗号化の手法としては、例えば、DES (Data Encryption Standard) や、FEAL (Fast Data Encipherment Algorithm) などを採用することができる。

【0167】

そして、管理者Aは、自身のリソースを、管理者B1に分け与えるとき、エリア中間キー $K_A$ を、管理者B1に与える。さらに、管理者Aは、管理者B1のエリアキー#0100hを決定し、自身のエリアコード#0000hとともに、管理者B1に与える（配布する）。

【0168】

従って、管理者B1は、エリア中間キー $K_A$ および自身のエリアキー#0100hを認識することができるが、システムキー、および、いわば親である管理者Aのエリアキー#0000hは認識することができない。但し、管理者B1のエリアキー#0100hは、親である管理者Aが、いわば子である管理者B1に与えたものであるから、親である管理者Aは、子である管理者B1のエリアキー#0100hを認識している。

【0169】

なお、管理者Aが管理者B1に与えたエリアキー#0100hは、管理者B1のエリア定義領域#0100hのエリア作成処理（図7）において、そのエリア定義領域#0100hに書き込まれる。

【0170】

管理者B1は、その親である管理者Aから得たエリア中間キー $K_A$ を、やはり管理者Aから得たエリアキー#0100hで暗号化し、エリア中間キー $K_{B1}$ を生成しておく。

【0171】

また、管理者Aは、自身のリソースを、管理者B2に分け与えるときも、エリア中間キー $K_A$ を、管理者B2に与える。さらに、管理者Aは、管理者B2のエリアキー#1000hを決定し、自身のエリアコード#0000hとともに、管

理者B2に与える。

【0172】

従って、管理者B2は、エリア中間キー $K_A$ および自身のエリアキー#1000hを認識することができるが、システムキー、および親である管理者Aのエリアキー#0000hは認識することができない。但し、管理者B2のエリアキー#1000hは、親である管理者Aが、子である管理者B2に与えたものであるから、親である管理者Aは、子である管理者B2のエリアキー#1000hを認識している。

【0173】

なお、管理者Aが管理者B2に与えたエリアキー#1000hは、管理者B2のエリア定義領域#1000hのエリア作成処理において、そのエリア定義領域#1000hに書き込まれる。

【0174】

管理者B2は、その親である管理者Aから得たエリア中間キー $K_A$ を、やはり管理者Aから得たエリアキー#1000hで暗号化し、エリア中間キー $K_{B2}$ を生成しておく。

【0175】

一方、管理者B1は、自身のリソースを、管理者Cに分け与えるとき、エリア中間キー $K_{B1}$ を、管理者Cに与える。さらに、管理者B1は、管理者Cのエリアキー#0300hを決定し、自身のエリアコード#0100hおよび親である管理者Aのエリアコード#0000hとともに、管理者Cに与える。

【0176】

従って、管理者Cは、エリア中間キー $K_{B1}$ および自身のエリアキー#0300hを認識することができるが、親である管理者B1のエリアキー#0100hは認識することができない。但し、エリアキー#0100hは、親である管理者B1が、子である管理者Cに与えたものであるから、親である管理者B1は、子である管理者Cのエリアキー#0300hを認識している。

【0177】

なお、管理者B1が管理者Cに与えたエリアキー#0300hは、管理者Cの

エリア定義領域#0300hのエリア作成処理において、そのエリア定義領域#0300hに書き込まれる。

#### 【0178】

管理者Cは、その親である管理者B1から得たエリア中間キーK<sub>B1</sub>を、やはり管理者B1から得たエリアキー#0300hで暗号化し、エリア中間キーK<sub>C</sub>を生成しておく。

#### 【0179】

そして、管理者Aは、自身のエリア定義領域#0000hの階層に作成されたサービス定義領域#0008hで管理されるサービス領域を利用してサービスを提供するとき、図10に示すように、サービス定義領域#0008hに記憶させたサービスキー（サービス定義領域#xxxxxhに記憶されたサービスキーを、以下、適宜、サービスキー#xxxxxhと記載する）を、エリア中間キーK<sub>A</sub>で暗号化し、サービス中間キーK<sub>#0008h</sub>を生成して、エリア中間キーK<sub>A</sub>とともに、サービス提供装置111に登録する。さらに、管理者Aは、自身のエリア定義領域#0000hのエリアコード#0000hと、そのエリア定義領域#0000hの階層に作成されたサービス定義領域#0008hのサービスコード#0008hも、サービス提供装置111に登録する。

#### 【0180】

ここで、サービス提供装置111は、例えば、図1のR/W1とコントローラ3から構成され、所定のサービス領域に対してデータを読み書きすることで、所定のサービスを提供するようになされている。

#### 【0181】

この場合、サービス提供装置111に、ICカード2が装着されると、サービス提供装置111とICカード2との間で、次のようにして相互認証が行われる。

#### 【0182】

即ち、サービス提供装置111は、図11に示すように、登録されているエリアコード#0000hと、サービスコード#0008hとを、ICカード2に送信する。ICカード2（シーケンサ91）では、サービス提供装置111からの

エリアコード#0000hおよびサービスコード#0008hが受信される。

#### 【0183】

そして、ICカード2では、システム定義ブロック（図4）に記憶されているシステムキーが読み出されるとともに、サービス提供装置111から受信したエリアコード#0000hを有するエリア定義領域からエリアキー#0000hが読み出される。さらに、システムキーが、エリアキー#0000hで暗号化され、その結果、図10のサービス提供装置111に登録されているエリア中間キー $K_A$ と同一のキーが生成される。このエリア中間キー $K_A$ と同一のキーは、認証に用いる第1アクセスキー（認証キー） $K_{bc}$ とされる。

#### 【0184】

また、ICカード2では、サービス提供装置111から受信したサービスコード#0008hを有するサービス定義領域からサービスキー#0008hが読み出される。そして、そのサービスキー#0008hで、エリア中間キー $K_A$ が暗号化され、その結果、図10のサービス提供装置111に登録されているサービス中間キー $K_{#0008h}$ と同一のキーが生成される。このサービス中間キー $K_{#0008h}$ と同一のキーは、認証に用いる第2アクセスキー $K_{ac}$ とされる。

#### 【0185】

従って、いまの場合、サービス提供装置111には、第1アクセスキー $K_{bc}$ または第2アクセスキー $K_{ac}$ であるエリア中間キー $K_A$ またはサービス中間キー $K_{#0008h}$ が登録されており、ICカード2では、第1アクセスキー $K_{bc}$ または第2アクセスキー $K_{ac}$ であるエリア中間キー $K_A$ またはサービス中間キー $K_{#0008h}$ が生成される。

#### 【0186】

そして、サービス提供装置111は、例えば、図12に示すようにして、ICカード2の認証を行う。

#### 【0187】

即ち、サービス提供装置111では、乱数が発生され、その乱数が、アルゴリズムE1にしたがって変換される。即ち、乱数が、第2アクセスキー $K_{ac}$ で暗号化（例えば、DES暗号化）され、その暗号化結果が、第1アクセスキー $K_{bc}$ で

復号（例えば、DES復号）される。さらに、その復号結果が、第2アクセスキーキー $K_{ac}$ で暗号化される。アルゴリズムE1による乱数の変換結果は、ICカード2に送信される。

## 【0188】

ICカード2では、サービス提供装置111からのアルゴリズムE1による乱数の変換結果が、アルゴリズムD1にしたがって変換される。即ち、アルゴリズムE1による変換結果が、第2アクセスキーキー $K_{ac}$ で復号され、その復号結果が、第1アクセスキーキー $K_{bc}$ で暗号化される。さらに、その暗号化結果が、第2アクセスキーキー $K_{ac}$ で復号される。

## 【0189】

そして、ICカード2では、アルゴリズムD1による変換結果が、さらに、アルゴリズムE2にしたがって変換される。即ち、アルゴリズムD1による変換結果が、第1アクセスキーキー $K_{bc}$ で暗号化される一方、第1アクセスキーキー $K_{bc}$ が、第2アクセスキーキー $K_{ac}$ で暗号化される。そして、アルゴリズムD1による変換結果の、第1アクセスキーキー $K_{bc}$ での暗号化結果が、第1アクセスキーキー $K_{bc}$ の、第2アクセスキーキー $K_{ac}$ での暗号化結果で復号される。さらに、その復号結果が、第1アクセスキーキー $K_{bc}$ で暗号化され、サービス提供装置111に送信される。

## 【0190】

サービス提供装置111では、ICカード2からのアルゴリズムE2による変換結果が、アルゴリズムD2にしたがって変換される。即ち、アルゴリズムE2による変換結果が、第1アクセスキーキー $K_{bc}$ で復号される一方、第1アクセスキーキー $K_{bc}$ が、第2アクセスキーキー $K_{ac}$ で暗号化される。そして、アルゴリズムE2による変換結果の、第1アクセスキーキー $K_{bc}$ での復号結果が、第1アクセスキーキー $K_{bc}$ の、第2アクセスキーキー $K_{ac}$ での暗号化結果で暗号化される。さらに、その暗号化結果が、第1アクセスキーキー $K_{bc}$ で復号される。

## 【0191】

そして、サービス提供装置111では、元の乱数と、アルゴリズムD2による変換結果とを比較することで、ICカード2の認証を行う。即ち、元の乱数と、アルゴリズムD2による変換結果とが一致している場合は、ICカード2が適正

なものとして認識され、一致していない場合は、ICカード2が不適正なもの（例えば、偽造されたもの）として認識される。

#### 【0192】

ICカード2が適正なものとして認識されると、ICカード2において、例えば、図13に示すようにして、サービス提供装置111の認証が行われる。

#### 【0193】

即ち、ICカード2では、乱数が発生され、その乱数が、アルゴリズムE2にしたがって変換され、サービス提供装置111に送信される。

#### 【0194】

サービス提供装置111では、ICカード2からのアルゴリズムE2による乱数の変換結果が、アルゴリズムD2にしたがって変換される。さらに、そのアルゴリズムD2による変換結果が、アルゴリズムE1にしたがって変換され、ICカード2に送信される。

#### 【0195】

ICカード2では、サービス提供装置111からのアルゴリズムE1による変換結果が、アルゴリズムD1にしたがって変換され、その変換結果と、元の乱数とを比較することで、サービス提供装置111の認証が行われる。即ち、元の乱数と、アルゴリズムD2による変換結果とが一致している場合は、サービス提供装置111が適正なものとして認識され、一致していない場合は、サービス提供装置111が不適正なもの（例えば、改造されたもの）として認識される。

#### 【0196】

ICカード2およびサービス提供装置111のいずれも適正なものと認められた場合、ICカード2では、サービス提供装置111から送信されてきたサービスコードを有するサービス定義領域によって管理されているサービス領域のみへのアクセスが許可される。従って、図10および図11で説明した場合においては、サービス定義領域#0008hで管理されているサービス領域のみへのアクセスが可能となる。

#### 【0197】

即ち、エリア中間キーKA、エリアコード#0000h、サービスキー#00

08 h、およびサービスコード#0008 hを知っている管理者Aは、サービス定義領域#0008 hで管理されているサービス領域にアクセスすることができる。但し、管理者Aは、サービスキー#1022 hや#030Chを知らないから、基本的に、サービス定義領域#1022 hや#030Chで管理されているサービス領域にアクセスすることはできない。

#### 【0198】

次に、管理者B2が、自身のエリア定義領域#1000 hの階層に作成されたサービス定義領域#1022 hで管理されるサービス領域を利用してサービスを提供するときは、図14に示すように、サービス定義領域#1022 hに記憶させたサービスキー#1022 hを、エリア中間キー $K_{B2}$ で暗号化し、サービス中間キー $K_{#1022h}$ を生成して、エリア中間キー $K_{B2}$ とともに、サービス提供装置111に登録する。そして、管理者B2は、自身のエリア定義領域#1000 hの階層より上位の階層のエリア定義領域のエリアコード、即ち、いまの場合、管理者Aのエリア定義領域#0000 hのエリアコード#0000 h、および自身のエリア定義領域#1000 hのエリアコード#1000 hと、そのエリア定義領域#1000 hの階層に作成されたサービス定義領域#1022 hのサービスコード#1022 hも、サービス提供装置111に登録する。

#### 【0199】

この場合、サービス提供装置111に、ICカード2が装着されると、サービス提供装置111とICカード2との間で、次のようにして相互認証が行われる。

#### 【0200】

即ち、サービス提供装置111は、図15に示すように、登録されているエリアコード#0000 hおよび#1000 hと、サービスコード#1022 hとを、ICカード2に送信する。ICカード2（シーケンサ91）では、サービス提供装置111からのエリアコード#0000 hおよび#1000 h、並びにサービスコード#1022 hが受信される。

#### 【0201】

そして、ICカード2では、システム定義ブロック（図4）に記憶されている

システムキーが読み出されるとともに、サービス提供装置111から受信したエリアコード#0000hまたは#1000hを有するエリア定義領域それぞれからエリアキー#0000hまたは#1000hが読み出される。さらに、システムキーが、エリアキー#0000hで暗号化され、その結果、エリア中間キー $K_A$ と同一のキーが生成される。そして、そのエリア中間キー $K_A$ と同一のキーが、エリアキー#1000hで暗号化され、その結果、図14のサービス提供装置111に登録されているエリア中間キー $K_{B2}$ と同一のキーが生成される。このエリア中間キー $K_{B2}$ と同一のキーは、認証に用いる第1アクセスキー $K_{bc}$ とされる。

#### 【0202】

また、ICカード2では、サービス提供装置111から受信したサービスコード#1022hを有するサービス定義領域からサービスキー#1022hが読み出される。そして、そのサービスキー#1022hで、エリア中間キー $K_{B2}$ と同一のキーが暗号化され、その結果、図14のサービス提供装置111に登録されているサービス中間キー $K_{#1022h}$ と同一のキーが生成される。このサービス中間キー $K_{#1022h}$ と同一のキーは、認証に用いる第2アクセスキー $K_{ac}$ とされる。

#### 【0203】

従って、いまの場合、サービス提供装置111には、第1アクセスキー $K_{bc}$ または第2アクセスキー $K_{ac}$ であるエリア中間キー $K_{B2}$ またはサービス中間キー $K_{#1022h}$ が登録されており、ICカード2では、第1アクセスキー $K_{bc}$ または第2アクセスキー $K_{ac}$ であるエリア中間キー $K_{B2}$ またはサービス中間キー $K_{#1022h}$ が生成される。

#### 【0204】

そして、ICカード2およびサービス提供装置111の間で、図12および図13で説明した場合と同様にして、相互認証が行われる。

#### 【0205】

その相互認証の結果、ICカード2およびサービス提供装置111のいずれも適正なものと認められた場合、ICカード2では、サービス提供装置111から送信されてきたサービスコードを有するサービス定義領域によって管理されているサービス領域のみへのアクセスが許可される。従って、図14および図15で

説明した場合においては、サービス定義領域#1022hで管理されているサービス領域のみへのアクセスが可能となる。

【0206】

即ち、エリア中間キーK<sub>B2</sub>、エリアコード#0000h、#1000h、サービスキー#1022h、並びにサービスコード#1022hを知っている管理者B2は、サービス定義領域#1022hで管理されているサービス領域にアクセスすることができる。但し、管理者B2は、サービスキー#0008hや#030Chを知らないから、基本的に、サービス定義領域#0008hや#030Chで管理されているサービス領域にアクセスすることはできない。

【0207】

次に、管理者Cが、自身のエリア定義領域#0300hの階層に作成されたサービス定義領域#030Chで管理されるサービス領域を利用してサービスを提供するときは、図16に示すように、サービス定義領域#030Chに記憶させたサービスキー#030Chを、エリア中間キーK<sub>C</sub>で暗号化し、サービス中間キーK<sub>#030Ch</sub>を生成して、エリア中間キーK<sub>C</sub>とともに、サービス提供装置111に登録する。そして、管理者Cは、自身のエリア定義領域#0300hの階層より上位の階層のエリア定義領域のエリアコード、即ち、いまの場合、管理者Aのエリア定義領域#0000hのエリアコード#0000hおよび管理者B1のエリア定義領域#0100hのエリアコード#0100h、並びに自身のエリア定義領域#0300hのエリアコード#0300hと、そのエリア定義領域#0300hの階層に作成されたサービス定義領域#030Chのサービスコード#030Chも、サービス提供装置111に登録する。

【0208】

この場合、サービス提供装置111に、ICカード2が装着されると、サービス提供装置111とICカード2との間で、次のようにして相互認証が行われる。

【0209】

即ち、サービス提供装置111は、図17に示すように、登録されているエリアコード#0000h、#0100h、および#0300hと、サービスコード

#030Chとを、ICカード2に送信する。ICカード2（シーケンサ91）では、サービス提供装置111からのエリアコード#0000h、#0100h、および#0300h、並びにサービスコード#030Chが受信される。

#### 【0210】

そして、ICカード2では、システム定義ブロック（図4）に記憶されているシステムキーが読み出されるとともに、サービス提供装置111から受信したエリアコード#0000h、#0100h、または#0300hを有するエリア定義領域それぞれからエリアキー#0000h、#0100h、または#0300hが読み出される。さらに、システムキーが、エリアキー#0000hで暗号化され、その結果、エリア中間キー $K_A$ と同一のキーが生成される。また、そのエリア中間キー $K_A$ と同一のキーが、エリアキー#0100hで暗号化され、その結果、エリア中間キー $K_{B1}$ と同一のキーが生成される。そして、そのエリア中間キー $K_{B1}$ と同一のキーが、エリアキー#0300hで暗号化され、その結果、図16のサービス提供装置111に登録されているエリア中間キー $K_C$ と同一のキーが生成される。このエリア中間キー $K_C$ と同一のキーは、認証に用いる第1アクセスキー $K_{bc}$ とされる。

#### 【0211】

また、ICカード2では、サービス提供装置111から受信したサービスコード#030Chを有するサービス定義領域からサービスキー#030Chが読み出される。そして、そのサービスキー#030Chで、エリア中間キー $K_C$ が暗号化され、その結果、図16のサービス提供装置111に登録されているサービス中間キー $K_{#030Ch}$ と同一のキーが生成される。このサービス中間キー $K_{#030Ch}$ と同一のキーは、認証に用いる第2アクセスキー $K_{ac}$ とされる。

#### 【0212】

従って、いまの場合、サービス提供装置111には、第1アクセスキー $K_{bc}$ または第2アクセスキー $K_{ac}$ であるエリア中間キー $K_C$ またはサービス中間キー $K_{#030Ch}$ がそれぞれ登録されており、ICカード2では、第1アクセスキー $K_{bc}$ または第2アクセスキー $K_{ac}$ であるエリア中間キー $K_C$ またはサービス中間キー $K_{#030Ch}$ がそれぞれ生成される。

【0213】

そして、ICカード2およびサービス提供装置111の間で、図12および図13で説明した場合と同様にして、相互認証が行われる。

【0214】

その相互認証の結果、ICカード2およびサービス提供装置111のいずれも適正なものと認められた場合、ICカード2では、サービス提供装置111から送信されてきたサービスコードを有するサービス定義領域によって管理されているサービス領域のみへのアクセスが許可される。従って、図16および図17で説明した場合においては、サービス定義領域#030Chで管理されているサービス領域のみへのアクセスが可能となる。

【0215】

即ち、エリア中間キーKC、エリアコード#0000h、#0100h、#0300h、サービスキー#030Ch、並びにサービスコード#030Chを知っている管理者Cは、サービス定義領域#030Chで管理されているサービス領域にアクセスすることができる。但し、管理者Cは、サービスキー#0008hや#1022Chを知らないから、基本的に、サービス定義領域#0008hや#1022Chで管理されているサービス領域にアクセスすることはできない。

【0216】

以上のように、上位の階層のエリアキーを知らなくても、管理者は、自身のサービス領域にアクセスすることができる。

【0217】

ところで、上述のように、各管理者は、サービスキーを知らないサービス定義領域によって管理されるサービス領域にはアクセスすることができないが、例えば、管理者Cが、自身のサービス定義領域#030Chによって管理されるサービス領域を利用したサービスの他、管理者B2のサービス定義領域#1022hによって管理されるサービス領域を利用したサービスも行いたい場合がある。

【0218】

この場合、管理者Cが、サービス定義領域#1022hによって管理されるサ

ービス領域にアクセスするには、図14および図15で説明したように、エリア中間キー $K_{B2}$ 、エリアコード#0000h、#1000h、サービスキー#1022h、並びにサービスコード#1022hを知る必要があり、従って、単純には、これらの情報を、管理者B2から教えてもらう必要がある。

#### 【0219】

しかしながら、管理者B2が知っているサービスキー#1022hは、その親である管理者Aでも知り得ないものであり、このような管理者B2しか知り得ないサービスキー#1022hを、管理者Cに教えてしまうのは、セキュリティの観点から好ましくない。

#### 【0220】

また、この場合、セキュリティの問題を無視しても、管理者Cが、サービス定義領域#030Chまたは#1022hによってそれぞれ管理される2つのサービス領域の両方にアクセスするには、ICカード2において、図15で説明した処理を行うことにより、第1アクセスキー $K_{bc}$ および第2アクセスキー $K_{ac}$ を生成し、サービス定義領域#030Chによって管理されるサービス領域へのアクセスのための相互認証を行うとともに、図17で説明した処理を行うことにより第1アクセスキー $K_{bc}$ および第2アクセスキー $K_{ac}$ を生成し、サービス定義領域#1022hによって管理されるサービス領域へのアクセスのための相互認証を行う必要がある。

#### 【0221】

従って、サービス領域ごとに、そのサービス領域へのアクセスのための相互認証を行う場合には、各サービス領域に、迅速にアクセスすることが困難となり、その結果、例えば、図1のカードシステムを駅の改札に通用した場合には、通勤者が、改札口に設けられているゲートを通過する、比較的に短い時間に、ICカード2の所定のサービス領域にアクセスして、データを書き込み、または読み出すことが困難となる。

#### 【0222】

そこで、例えば、管理者Cが、自身のサービス定義領域#030Chによって管理されるサービス領域を利用したサービスの他、管理者B2のサービス定義領

域#1022hによって管理されるサービス領域を利用したサービスも行う場合には、セキュリティの問題を解決し、かつサービス領域への迅速なアクセスを確保するために、管理者CおよびB2との間で、例えば、図18に示すような、情報のやりとりを行い、サービス提供装置111への登録を行う。

#### 【0223】

即ち、管理者Cは、図16における場合と同様に、サービス定義領域#030Chに記憶させたサービスキー#030Chを、エリア中間キーKCで暗号化し、サービス中間キーK<sub>#030Ch</sub>を生成する。さらに、管理者Cは、このサービス中間キーK<sub>#030Ch</sub>を、管理者B2に渡し、サービスキー#1022hで暗号化してもらう。そして、管理者Cは、サービス中間キーK<sub>#030Ch</sub>の、サービスキー#1022hでの暗号化結果であるサービス中間キーK<sub>#1022h</sub>を、サービスコード#1022hとともに受け取る。

#### 【0224】

従って、管理者CとB2との間でやりとりされるキーは、サービス中間キーK<sub>#030Ch</sub>およびK<sub>#1022h</sub>だけであり、管理者Cしか知り得ないサービスキー#030Chが、管理者B2に知られたり、また、管理者B2しか知り得ないサービスキー#1022hが、管理者Cに知られることはない。即ち、セキュリティ上の問題はない。

#### 【0225】

管理者B2から、サービス中間キーK<sub>#1022h</sub>およびサービスコード#1022hを受け取った管理者Cは、それらとともに、自身のエリア定義領域#0300hの階層より上位の階層のエリア定義領域のエリアコード、即ち、いまの場合、管理者Aのエリア定義領域#0000hのエリアコード#0000hおよび管理者B1のエリア定義領域#0100hのエリアコード#0100h、並びに自身のエリア定義領域#0300hのエリアコード#0300hを、サービス提供装置111に登録する。さらに、管理者Cは、エリア中間キーKC、およびエリア定義領域#0300hの階層に作成されたサービス定義領域#030Chのサービスコード#030Chも、サービス提供装置111に登録する。

## 【0226】

この場合、サービス提供装置111に、ICカード2が装着されると、サービス提供装置111とICカード2との間で、次のようにして相互認証が行われる。

## 【0227】

即ち、サービス提供装置111は、図19に示すように、登録されているエリアコード#0000h、#0100h、および#0300hと、サービスコード#030Chおよび#1022hとを、ICカード2に送信する。ICカード2（シーケンサ91）では、サービス提供装置111からのエリアコード#0000h、#0100h、および#0300h、並びにサービスコード#030Chおよび#1022hが受信される。

## 【0228】

そして、ICカード2では、システム定義ブロック（図4）に記憶されているシステムキーが読み出されるとともに、サービス提供装置111から受信したエリアコード#0000h、#0100h、または#0300hを有するエリア定義領域それぞれからエリアキー#0000h、#0100h、または#0300hが読み出され、図17で説明した場合と同様にして、図18のサービス提供装置111に登録されているエリア中間キー $K_C$ と同一のキーが生成される。このエリア中間キー $K_C$ と同一のキーは、認証に用いる第1アクセスキー $K_{bc}$ とされる。

## 【0229】

また、ICカード2では、サービス提供装置111から受信したサービスコード#030Chまたは#1022hを有するサービス定義領域それぞれからサービスキー#030Chまたは#1022hが読み出される。そして、まず、サービスキー#030Chで、エリア中間キー $K_C$ が暗号化され、その結果、サービス中間キー $K_{#030Ch}$ と同一のキーが生成される。さらに、そのサービス中間キー $K_{#030Ch}$ と同一のキーが、サービスキー#1022hで暗号化され、図18のサービス提供装置111に登録されているサービス中間キー $K_{#1022h}$ と同一のキーが生成される。このサービス中間キー $K_{#1022h}$ と同一のキーは、認証に用い

る第2アクセスキー $K_{ac}$ とされる。

#### 【0230】

従って、いまの場合、サービス提供装置111には、第1アクセスキー $K_{bc}$ または第2アクセスキー $K_{ac}$ であるエリア中間キー $K_C$ またはサービス中間キー $K_{\#1022h}$ が登録されており、ICカード2では、第1アクセスキー $K_{bc}$ または第2アクセスキー $K_{ac}$ であるエリア中間キー $K_C$ またはサービス中間キー $K_{\#1022h}$ が生成される。

#### 【0231】

そして、ICカード2およびサービス提供装置111の間で、図12および図13で説明した場合と同様にして、相互認証が行われる。

#### 【0232】

その相互認証の結果、ICカード2およびサービス提供装置111のいずれも適正なものと認められた場合、ICカード2では、サービス提供装置111から送信されてきたサービスコードを有するサービス定義領域によって管理されているサービス領域のみへのアクセスが許可される。従って、図18および図19で説明した場合においては、サービス定義領域#030Chで管理されているサービス領域、およびサービス定義領域#1022Chで管理されているサービス領域へのアクセスが可能となる。

#### 【0233】

以上のように、システムキーを、2以上のエリアキーまたはサービスキーで暗号化することにより、その2以上のエリアキーまたはサービスキーを、2つの第1アクセスキー $K_{bc}$ および第2アクセスキー $K_{ac}$ に縮退（合成）し、その第1アクセスキー $K_{bc}$ および第2アクセスキー $K_{ac}$ を用いて、サービス提供装置111から送信されてきたサービスコードを有するサービス定義領域によって管理されているサービス領域へのアクセスを許可するための相互認証を行うようにしたので、複数のサービス定義領域へのアクセスを対象とする場合でも、短時間で、相互認証を終了することができ、これにより、サービス領域への迅速なアクセスを確保することができる。

## 【0234】

なお、図12および図13で説明した場合には、相互認証処理を、第1アクセスキーキー $K_{bc}$ および第2アクセスキーキー $K_{ac}$ の2つのキーを用いて行うようにしたが、例えば、第2アクセスキーキー $K_{ac}$ だけを用いて行うようにすることも可能である。この場合、ICカード2では、システムキーを、2以上のエリアキーまたはサービスキーで暗号化することにより、その2以上のエリアキーまたはサービスキーが、1の第2アクセスキーキー $K_{ac}$ に縮退されることになる。

## 【0235】

また、相互認証には、図20に示すように、第1アクセスキーキー $K_{bc}$ および第2アクセスキーキー $K_{ac}$ を、ICカード2に固有の値である、例えば、製造IDブロックに記憶された製造IDなどで暗号化した暗号化結果を用いることも可能である。ここで、図20においては、第1アクセスキーキー $K_{bc}$ については、製造IDとのEXORをとられることで暗号化が行われており、第2アクセスキーキー $K_{ac}$ については、DES方式による暗号化が行われている。なお、第2アクセスキーキー $K_{ac}$ については、第1アクセスキーキー $K_{bc}$ と製造IDとのEXORの結果をキーとして、DES方式による暗号化を行うことも可能である。

## 【0236】

このように、第1アクセスキーキー $K_{bc}$ および第2アクセスキーキー $K_{ac}$ を暗号化した暗号化結果を相互認証に用いる場合には、セキュリティを、より向上させることが可能となる。なお、この場合、サービス提供装置111において、製造IDが必要となるが、これは、ICカード2から送信するようにすれば良い。

## 【0237】

次に、EEPROM66の記憶領域が、エリア定義領域を階層とする階層構造をなしており、さらに、各エリア定義領域およびサービス定義領域が、認証のためのエリアキーおよびサービスキーを記憶するようになされている結果、例えば、次のような、フレキシビリティのあるアクセス制御を行うことができる。

## 【0238】

即ち、例えば、ある管理者を、親の管理者として、そのリソースを分け与えられた子の管理者が、不正なサービスなどを行っており、そのサービスの提供を停

止させたい場合には、親の管理者が、そのエリア定義領域に記憶されたエリアキーを変更することで、子の管理者による、ICカード2へのアクセスを禁止することができる。

#### 【0239】

具体的には、例えば、図5において、管理者B1が、管理者Cによるサービスの提供を停止させる場合、ICカード2のエリア定義領域#0100hに記憶されたエリアキー#0100hを変更する。この場合、図17において、ICカード2において生成されるエリア中間キー $K_{B1}$ 、さらには、エリア中間キー $K_C$ も変更されることとなるから、変更前のエリア中間キー $K_C$ しか知らない管理者Cは、サービス定義領域#030Chにアクセスすることはできなくなる。

#### 【0240】

なお、管理者Cの親の管理者である管理者B1の、さらに親の管理者である管理者Aが、そのエリア定義領域#0000hに記憶されたエリアキー#0000hを変更することによっても、サービス定義領域#030Chへのアクセスを禁止することが可能である。但し、この場合は、管理者Aの子の管理者B2が、自身のサービス定義領域#1022hによって管理されるサービス領域にアクセスすることもできなくなる。即ち、ある管理者が、そのエリアキーを変更した場合には、そのエリア定義領域の階層の中にある階層（子の階層、孫の階層、・・・）のエリア定義領域が管理しているサービス定義領域へのアクセスはできなくなる。

#### 【0241】

また、図18および図19では、管理者Cが、管理者B2のサービス定義領域#1022h（によって管理されるサービス領域）を、管理者B2と共有する場合について説明したが、キーの管理によっては、管理者どうしの間で、より複雑な関係のサービス定義領域の共有が可能となる。

#### 【0242】

具体的には、例えば、いま、EEPROM66において、図21に示すような階層構造が構成されているとする。即ち、図21では、ICカード2の発行者でもある管理者Aのエリア定義領域#0000hの階層の子の階層として、管理者

Eのエリア定義領域#5000h、および管理者Gのエリア定義領域#7000hが作成されている。さらに、管理者Eのエリア定義領域#5000hの階層には、サービス定義領域#5008h、#5048h、#5088h、および#50C8hが作成されるとともに、管理者Fのエリア定義領域#6000hが作成されている。

#### 【0243】

また、管理者Fのエリア定義領域#6000hの階層には、サービス定義領域#6008hおよび#6048hが作成されており、管理者Gのエリア定義領域#7000hの階層には、サービス定義領域#7008hおよび#70C8hが作成されている。

#### 【0244】

以上のような階層構造において、管理者Aは、図22（A）に示すように、システムキーを、エリアキー#0000hで暗号化し、その暗号化結果を、子の管理者である管理者EおよびGに渡す。

#### 【0245】

管理者Eは、図22（B）に示すように、管理者Aからの、システムキーの、エリアキー#0000hでの暗号化結果を、エリアキー#5000hで暗号化し、その暗号化結果を、第1アクセスキーキー $K_{E1}$ として用いることとする。さらに、管理者Eは、第1アクセスキーキー $K_{E1}$ （エリアキー#5000hによる暗号化結果）を、サービスキー#5008h、#5048h、#5088h、#50C8hで順次暗号化し、その最終的な暗号化結果を、第2アクセスキーキー $K_{E2}$ として用いることとする。

#### 【0246】

また、管理者Fは、図22（C）に示すように、管理者Eから第1アクセスキーキー $K_{E1}$ （エリアキー#5000hによる暗号化結果）をもらい、それを、エリアキー#6000hで暗号化し、その暗号化結果を、第1アクセスキーキー $K_{F1}$ とする。さらに、管理者Fは、第1アクセスキーキー $K_{F1}$ （エリアキー#6000hによる暗号化結果）を、サービスキー#6008h、#6048hで順次暗号化する。そして、その暗号化結果を、管理者Eに渡し、サービスキー#5048h、#5

088 hで順次暗号化してもらう。その後、管理者Fは、その暗号化結果を、管理者Eからもらい、管理者Gに渡し、サービスキー#70C8 hで暗号化してもらう。そして、管理者Fは、その暗号化結果を、管理者Gからもらい、第2アクセスキー $K_{F2}$ として用いることとする。

#### 【0247】

一方、管理者Gは、図22(D)に示すように、管理者Aからの、システムキーの、エリアキー#0000 hでの暗号化結果を、エリアキー#7000 hで暗号化し、その暗号化結果を、第1アクセスキー $K_{G1}$ として用いることとする。さらに、管理者Gは、第1アクセスキー $K_{G1}$ （エリアキー#7000 hによる暗号化結果）を、サービスキー#7008 h、#70C8 hで順次暗号化し、その最終的な暗号化結果を、管理者Fに渡して、サービスキー#6048 hで暗号化してもらう。その後、管理者Gは、管理者Fによるサービスキー#6048を用いた暗号化結果を、管理者Eに渡し、サービスキー#5088 h、#50C8 hで順次暗号化してもらう。そして、管理者Gは、その暗号化結果を、管理者Eからもらい、第2アクセスキー $K_{G2}$ として用いることとする。

#### 【0248】

この場合、ICカード2において、図22で説明した場合と同様の手順で、EEPROM66に記憶されているエリアキー、サービスキーを用いて、システムキーを暗号化し、第1アクセスキーおよび第2アクセスキーを生成することで、管理者E、F、G相互の間では、図23に示すようなサービス定義領域の共有が可能となる。

#### 【0249】

即ち、管理者Eは、自身のサービス定義領域#5008、#5048 h、#5088 h、#50C8 hのみにアクセスすることができる。管理者Fは、自身のサービス定義領域#6008 h、#6048 hにアクセスする他、管理者Eのサービス定義領域#5048 h、#5088 h、および管理者Gのサービス定義領域#70C8 hにアクセスすることが可能となる。管理者Gは、自身のサービス定義領域#7008 h、#70C8 hにアクセスする他、管理者Eのサービス定義領域#5088 h、#50C8 h、および管理者Fのサービス定義領域#60

48hにアクセスすることが可能となる。

#### 【0250】

なお、図22に示したようなキーの受け渡しにおいて、ある管理者のサービスキー自身が、他の管理者に知られることはない。即ち、管理者Eのサービスキー#5008h、#5048h、#5088h、#50C8hは、親の管理者Aは勿論、管理者FおよびGにも知られることはない。同様に、管理者Fのサービスキー#6008h、#6048hは、管理者EおよびGに知られることはなく、管理者Gのサービスキー#7008h、#70C8hは、管理者EおよびFに知られることはない。

#### 【0251】

また、上述したように、ある管理者が、そのエリアキーを変更した場合には、そのエリア定義領域の階層の中にある階層のエリア定義領域が管理しているサービス定義領域すべてへのアクセスはできなくなるが、即ち、親の管理者がエリアキーを変更した場合には、その子の管理者は、ICカード2へのアクセスをすることができなくなるが、キー管理の仕方によっては、特定の子の管理者だけのアクセスを禁止することが可能となる。

#### 【0252】

具体的には、例えば、いま、EEPROM66において、図24に示すような階層構造が構成されているとする。即ち、図24では、ICカード2の発行者でもある管理者Aのエリア定義領域#0000hの階層の子の階層として、管理者Hのエリア定義領域#8000h、管理者Iのエリア定義領域#9000h、および管理者Jのエリア定義領域#A000hが作成されている。さらに、管理者Hのエリア定義領域#8000hの階層には、サービス定義領域#8008h、#8104h、および#8105hが作成されている。

#### 【0253】

以上のような階層構造において、管理者Aは、図25(A)に示すように、システムキーを、エリアキー#0000hで暗号化し、その暗号化結果を、子の管理者である管理者IおよびJに渡す。

## 【0254】

管理者Iは、図25(C)に示すように、管理者Aからの、システムキーの、エリアキー#0000hでの暗号化結果を、エリアキー#9000hで暗号化し、その暗号化結果を、第1アクセスキーK<sub>I1</sub>として用いることとする。さらに、管理者Iは、第1アクセスキーK<sub>I1</sub>(エリアキー#9000hによる暗号化結果)を、管理者Hに渡し、図25(B)に示すように、サービスキー#8008h、#8104hで順次暗号化してもらう。そして、管理者Iは、その暗号化結果を、図25(C)に示すように、第2アクセスキーK<sub>I2</sub>として用いることとする。

## 【0255】

また、管理者Jは、図25(D)に示すように、管理者Aからの、システムキーの、エリアキー#0000hでの暗号化結果を、エリアキー#A000hで暗号化し、その暗号化結果を、第1アクセスキーK<sub>J1</sub>として用いることとする。さらに、管理者Jは、第1アクセスキーK<sub>J1</sub>(エリアキー#A000hによる暗号化結果)を、管理者Hに渡し、図25(B)に示すように、サービスキー#8008h、#8105hで順次暗号化してもらう。そして、管理者Jは、その暗号化結果を、図25(D)に示すように、第2アクセスキーK<sub>J2</sub>として用いることとする。

## 【0256】

この場合、ICカード2において、図25で説明した場合と同様の手順で、EEPROM66に記憶されているエリアキー、サービスキーを用いて、システムキーを暗号化し、第1アクセスキーおよび第2アクセスキーを生成することで、管理者Iは、管理者Hのサービス定義領域#8008hおよび#8104hにアクセスすることが、管理者Jは、管理者Hのサービス定義領域#8008hおよび#8105hにアクセスすることが、それぞれ可能となる。

## 【0257】

一方、管理者Hは、サービス定義領域#8008hを、管理者IおよびJとの間でデータを共有するものとして作成しておき、サービス定義領域#8104hまたは#8105hを、管理者IまたはJそれぞれによるサービス定義領域#8

008 hへのアクセスを制御するための、いわばダミーのサービス定義領域として作成しておく。従って、サービス定義領域 #8104 hおよび#8105 hで管理されるサービス領域は必要なく、その容量は0ブロックで良い。

#### 【0258】

この場合において、管理者Hが、例えば、サービスキー #8104 hを変更すると、ICカード2において、そのサービスキー #8104 hを用いて、第2アクセスキー  $K_{I2}$  が生成されて認証が行われる管理者Iは、サービス定義領域 #8008 hにアクセスすることができなくなる。即ち、管理者Iによるサービス定義領域 #8008 hへのアクセスだけが禁止される。一方、管理者Hが、例えば、サービスキー #8105 hを変更すると、ICカード2において、そのサービスキー #8105 hを用いて、第2アクセスキー  $K_{J2}$  が生成されて認証が行われる管理者Jは、サービス定義領域 #8008 hにアクセスすることができなくなる。即ち、管理者Jによるサービス定義領域 #8008 hへのアクセスだけが禁止される。

#### 【0259】

以上のように、ダミーのサービス定義領域を利用して、特定の子の管理者だけのアクセスを禁止することができる。

#### 【0260】

次に、図6で説明したように、管理者が、エリア定義領域やサービス定義領域を作成するのに必要な、コード範囲や、割り当てブロック数、エリアキー、サービスキーなどの、ユーザブロックを管理するための管理情報（以下、適宜、発券情報ともいう）を、発券機101に登録し、発券作業が行われる場合において、発券機101が、例えば、駅や、小売店、その他の安全でない場所に設置されているときには、前述したように、盗聴や改竄等の不正行為が行われる蓋然性の高く、セキュリティ管理上好ましくない。

#### 【0261】

そこで、ここでは、図26に示すように、エリア定義領域やサービス定義領域を作成しようとする管理者（以下、適宜、発券業者という）が、発券情報を暗号化し、その暗号化された発券情報を、例えば、公衆回線やインターネット、地上

波、衛星回線、CATV (Cable Television) 線などの伝送媒体121を介して、発券機101に伝送して登録するようにしている。そして、発券機101では、ICカード2に、暗号化された発券情報が送信され、さらに、ICカード2では、その暗号化された発券情報が復号され、エリア定義領域やサービス定義領域の作成が行われるようになされている。

#### 【0262】

ここで、図26は、管理者#1がサービスを提供するための記憶領域だけが構成されていたICカード2に、上述のようにして、管理者#2がサービスを提供するための記憶領域が構成された状態（発券作業が行われた状態）を示している。

#### 【0263】

次に、図27は、以上のような発券作業を行う発券処理システムの一実施の形態の構成例を示している。

#### 【0264】

発券情報提供装置131は、後述する発券情報提供処理を行うことで、暗号化された発券情報（以下、適宜、暗号化発券情報という）を、伝送媒体121を介して、発券機101に送信する。発券機101は、発券情報提供装置131からの暗号化発券情報を受信して登録する。そして、発券機101は、ICカード2が装着されると、暗号化発券情報を、ICカード2に送信する。ICカード2は、発券機101から暗号化発券情報を受信し、後述する復号処理を行うことで、暗号化発券情報を、元の発券情報に復号する。そして、ICカード2は、上述のエリア作成処理（図7）またはサービス作成処理（図8）を行うことで、復号した発券情報に基づき、エリア定義領域またはサービス定義領域をそれぞれ作成する。

#### 【0265】

次に、図28のフローチャートを参照して、発券情報提供装置131が行う発券情報提供処理について説明する。

#### 【0266】

発券情報提供装置131には、エリア定義領域を作成するのに必要な、例えば

、コード範囲、割り当てブロック数、エリアキー、またはサービス定義領域を作成するのに必要な、例えば、サービスコード、割り当てブロック数、サービスキーが入力される。そして、ステップS21において、これらの入力情報に基づいて、発券情報が作成される。

#### 【0267】

即ち、エリア定義領域を作成するのに必要なコード範囲、割り当てブロック数、エリアキーが入力された場合には、それらを対応付けることで、発券情報が作成される。また、サービス定義領域を作成するのに必要なサービスコード、割り当てブロック数、サービスキーが入力された場合には、それらを対応付けることで、発券情報が作成される。

#### 【0268】

そして、ステップS22に進み、ステップS21で作成された発券情報について、例えば、誤り訂正符号が演算され、これが、改竄をチェックするためのチェックコードとして、発券情報に含められる。

#### 【0269】

その後、ステップS23において、発券情報が暗号化される。即ち、ステップS23では、例えば、発券情報によって作成しようとしているエリア定義領域またはサービス定義領域の親の階層のエリア定義領域のエリアキーで、その発券情報が暗号化され、暗号化発券情報とされる。

#### 【0270】

そして、ステップS24に進み、暗号化発券情報に対し、そのヘッダとして、識別コード（暗号化発券情報が、エリア定義領域を作成するためのものである場合には、そのエリアコードであり、サービス定義領域を作成するためのものである場合には、そのサービスコード）が付加され、伝送媒体121を介して、発券機101に送信されて、発券情報提供処理を終了する。

#### 【0271】

従って、例えば、図5において、親の管理者Aが、子の管理者B1のエリア定義領域#0100hを作成する場合には、図29(A)に示すような暗号化発券情報が、発券情報提供装置131から送信される。即ち、図29(A)の暗号化

発券情報の先頭には、ヘッダとして、エリア定義領域#0100hのエリアコード#0100hが配置されている。なお、このエリアコード#0100hは、ICカード2において、親の階層を認識するために、暗号化されていない。また、発券情報提供装置131において、エリアコード#0100hは、入力情報のうちのコード範囲から認識される。これは、上述したように、本実施の形態では、エリア定義領域については、そのコード範囲の最小値が、エリアコードとされるため、エリアコードは、コード範囲から認識することができるからである。

#### 【0272】

暗号化されていない、ヘッダとしてのエリアコード#0100hの後には、エリア定義領域#0100hに記憶させるべきコード範囲#0100h - #03FFh、割り当てブロック数33、エリアキー#0100hとしてのa0a0a0a0a0a0a0a0a0、チェックコードが順次配置されている。そして、これらは、親の階層であるエリア定義領域#0000hのエリアキー#0000hとしての0123456789abcdefで暗号化（図29（A）において影を付して示す）されている。

#### 【0273】

また、例えば、図5において、管理者B2が、自身のサービス定義領域#1022hを作成する場合には、図29（B）に示すような暗号化発券情報が、発券情報提供装置131から送信される。即ち、図29（B）の暗号化発券情報の先頭には、ヘッダとして、サービス定義領域#1022hのサービスコード#1022hが配置されている。なお、このサービスコード#1022hは、ICカード2において、親の階層（サービス定義領域が属する階層）を認識するために、暗号化されていない。

#### 【0274】

暗号化されていない、ヘッダとしてのサービスコード#1022hの後には、サービス定義領域#1022hに記憶させるべきサービスコード#1022h、割り当てブロック数5、エリアキー#1022hとしての0303030303030303、チェックコードが順次配置されている。そして、これらは、親の階層であるエリア定義領域#1000hのエリアキー#1000hとしてのc0c0c0c0c0c0c0c0で暗号化（図29（B）において影を付して示す）されている。

## 【0275】

以上のように、発券情報は、親の階層のエリアキーで暗号化されるため、そのエリアキーを知らない限り、発券情報の内容も知ることができない。従って、そのような暗号化発券情報を、安全でない場所に送信しても、その内容の漏洩を防止することができる。さらに、その結果、例えば、暗号化発券情報を、第三者に配布して、発券機101への登録や、ICカード2への送信などを依頼することが可能となる。

## 【0276】

なお、ここでは、発券情報を、親の階層のエリアキーで暗号化することとしているため、発券情報提供処理は、基本的に、その親の管理者の下で行うのが望ましい。即ち、第三者に、発券情報提供処理を行わせる場合には、暗号化に用いる親の階層のエリアキーを、その第三者に公開しなければならず、セキュリティ上好ましくないため、発券情報提供処理は、親の管理者の下で行うのが望ましい。

## 【0277】

次に、図30のフローチャートを参照して、ICカード2が行う復号処理について説明する。

## 【0278】

上述したように、発券機101は、発券情報提供装置131から、暗号化発券情報が送信されると、それを受信して登録する。そして、発券機101は、ICカード2が装着されると、暗号化発券情報を、ICカード2に送信する。ICカード2は、発券機101から暗号化発券情報を受信し、ステップS31において、その暗号化発券情報によって作成するエリア定義領域またはサービス定義領域の親の階層としてのエリア定義領域を認識する。

## 【0279】

即ち、ステップS31では、暗号化発券情報のヘッダを参照することで、作成対象のエリア定義領域またはサービス定義領域のエリアコードまたはサービスコードが認識される。さらに、ステップS31では、その認識されたエリアコードまたはサービスコードを、コード範囲に含むエリア定義領域が、EEPROM66から検出され、そのエリア定義領域が、親の階層として認識される。

## 【0280】

そして、ステップS32に進み、ステップS31で認識された親の階層のエリア定義領域に記憶されているエリアキーで、暗号化発券情報が復号され、ステップS33に進む。ステップS33では、復号された発券情報に含まれるチェックコードに基づいて、その発券情報の改竄が行われているか否かが判定される。ステップS33において、発券情報の改竄が行われていると判定された場合、ステップS34に進み、発券情報の改竄が行われている旨のメッセージを、発券機101に送信し、また、復号された発券情報を破棄するなどのエラー処理が行われ、復号処理を終了する。この場合、復号処理は異常終了し、エリア定義領域やサービス定義領域は作成されない。

## 【0281】

一方、ステップS33において、発券情報の改竄が行われていないと判定された場合、復号処理を終了する。この場合、復号処理は正常終了し、その後、復号された発券情報をEEPROM66に記憶させる処理、即ち、エリア定義領域またはサービス定義領域を作成するエリア作成処理（図7）またはサービス作成処理（図8）が行われる。

## 【0282】

なお、発券情報が改竄されているか否かのチェックは、チェックコードによる他、暗号化発券情報のヘッダを用いて行うことも可能である。即ち、暗号化発券情報が、エリア定義領域を作成するためのものであれば、図29（A）に示したように、そのヘッダには、エリアコードが配置され、そのエリアコードは、その後に配置された、暗号化されたコード範囲の最小値に一致しているはずである。従って、ヘッダに配置されたエリアコードと、その後に配置されたコード範囲の最小値とを比較することで、暗号化発券情報の改竄の有無をチェックすることができる。また、暗号化発券情報が、サービス定義領域を作成するためのものであれば、図29（B）に示したように、そのヘッダには、サービスコードが配置され、そのサービスコードは、その後に配置された、暗号化されたサービスコードに一致しているはずである。従って、ヘッダに配置されたサービスコードと、その後に配置されたサービスコードとを比較することで、暗号化発券情報の改竄の

有無をチェックすることができる。

#### 【0283】

以上のように、発券情報提供装置131において、発券情報を暗号化して、暗号化発券情報とし、ICカード2において、その暗号化発券情報を復号するようにしたので、発券機101を安全でない場所に設置し、伝送媒体121を介して伝送しても、盗聴や改竄等の不正行為が行われることを防止することができる。

#### 【0284】

その結果、ICカード2を利用して新たなサービスの提供を開始するために発券作業を行う場合に、ICカード2を回収する必要がなくなり、従って、その回収に要するコストの削減を図ることができる。また、ICカード2のユーザからすれば、新たなサービスの提供が開始された場合に、ICカード2を回収してもらわなくても、発券機101が設定されている場所に、ICカード2を持っていき、発券作業を行うことで、その新たなサービスの提供を受けることが、即座に可能となる。

#### 【0285】

以上、本発明を、非接触で通信が行われる非接触カードシステムに適用した場合について説明したが、本発明は、接触した状態で通信が行われるカードシステムにも適用可能である。また、本発明の適用範囲は、カードシステムに限定されるものではない。

#### 【0286】

なお、本実施の形態では、認証を、いわゆる秘密鍵方式で行うようにしたが、認証は、いわゆる公開鍵方式で行うようにすることも可能である。

#### 【0287】

また、本実施の形態では、あるエリア定義領域の階層のサービス定義領域にアクセスするときに、そのエリア定義領域の階層から、最上位階層までのパス上にあるエリア定義領域のエリアキーを順次用いて、第1アクセスキーを生成するようにしたが、第1アクセスキーの生成方法は、これに限定されるものではない。さらに、本実施の形態では、アクセス対象のサービス定義領域のサービスキーを順次用いて、第2アクセスキーを生成するようにしたが、第2アクセスキーの生

成方法も、これに限定されるものではない。即ち、第1アクセスキーおよび第2アクセスキーは、任意の2以上のエリアキーまたはサービスキーを順次用いて生成することが可能である。

## 【0288】

さらに、本実施の形態では、ユーザブロックおよびシステムブロックのいずれも、1のメモリであるEEPROM66に記憶させるようにしたが、ユーザブロックとシステムブロックとは、物理的に、別々のメモリに記憶させるようにすることが可能である。

## 【0289】

また、本実施の形態では、データをEEPROMに記憶させるようにしたが、データは、EEPROM以外の半導体メモリや、磁気ディスクなどに記憶させることも可能である。

## 【0290】

さらに、本実施の形態では、発券情報提供処理において、親の階層のエリア定義領域におけるエリアキーで、発券情報を暗号化するようにしたが、発券情報の暗号化に用いるキーは、そのような親の階層のエリアキーに限定されるものではない。但し、ICカード2において、暗号化発券情報を復号する必要があることから、発券情報の暗号化に用いるキーは、ICカード2に記憶させておく必要がある。従って、親の階層のエリアキーを、発券情報の暗号化に用いる場合には、その親の階層のエリアキーは、既に、ICカード2に記憶されているから、それとは別に、発券情報の復号（暗号化）に用いるキーを、ICカード2に記憶させる必要はない。

## 【0291】

また、本実施の形態では、EEPROM66の記憶領域を階層構造にして管理するようにしたが、本発明は、EEPROM66の記憶領域が階層構造で管理されていない場合にも適用可能である。

## 【0292】

さらに、本実施の形態では、暗号化発券情報を、伝送媒体121を介して、発券機101に送信して登録するようにしたが、暗号化発券情報は、例えば、磁気

ディスクや、光磁気ディスク、光ディスク、メモリカード、磁気テープなどの記録媒体（記憶媒体）に記憶させ、それを、直接、発券機101を持っていくことで登録することも可能である。

【0293】

【発明の効果】

請求項1に記載の情報処理装置および請求項5に記載の情報処理方法によれば、データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報が暗号化される。従って、管理情報の内容が第三者に知られることを防止することが可能となる。

【0294】

請求項6に記載の情報処理装置および請求項10に記載の情報処理方法によれば、データ記憶手段の記憶領域を管理するための、その記憶領域にアクセスするのに必要なキーを含む管理情報であって、暗号化されたものが復号される。従つて、管理情報の内容が第三者に知られることを防止することが可能となる。

【図面の簡単な説明】

【図1】

本発明を適用したICカードを用いたカードシステムの一実施の形態の構成例を示すブロック図である。

【図2】

図1のリーダ／ライタ1の構成例を示すブロック図である。

【図3】

図1のICカード2の構成例を示すブロック図である。

【図4】

図3のEEPROM66の論理フォーマットを示す図である。

【図5】

図3のEEPROM66のディレクトリ構造を示す図である。

【図6】

図5の階層構造が構成されていく過程を説明するための図である。

【図7】

エリア作成処理を説明するためのフローチャートである。

【図8】

サービス作成処理を説明するためのフローチャートである。

【図9】

管理者間でのキーの受け渡しを説明するための図である。

【図10】

管理者Aがサービスを提供するときに必要な情報を説明するための図である。

【図11】

管理者Aがサービスを提供するときのICカード2の処理を説明するための図である。

【図12】

サービス提供装置111によるICカード2の認証方法を説明するための図である。

【図13】

ICカード2によるサービス提供装置111の認証方法を説明するための図である。

【図14】

管理者B2がサービスを提供するときに必要な情報を説明するための図である

【図15】

管理者B2がサービスを提供するときのICカード2の処理を説明するための図である。

【図16】

管理者Cがサービスを提供するときに必要な情報を説明するための図である。

【図17】

管理者Cがサービスを提供するときのICカード2の処理を説明するための図である。

【図18】

管理者Cがサービスを提供するときに必要な情報を説明するための図である。

【図19】

管理者Cがサービスを提供するときのICカード2の処理を説明するための図である。

【図20】

相互認証に用いる第1アクセスキーおよび第2アクセスキーの生成方法を説明するための図である。

【図21】

E PROM66における階層構造を示す図である。

【図22】

管理者間でのキーの受け渡しを説明するための図である。

【図23】

管理者間でのサービス(データ)の共有を説明するための図である。

【図24】

E PROM66における階層構造を示す図である。

【図25】

管理者間でのキーの受け渡しを説明するための図である。

【図26】

本発明の原理を説明するための図である。

【図27】

本発明を適用した発券処理システムの一実施の形態の構成例を示すブロック図である。

【図28】

発券情報提供処理を説明するためのフローチャートである。

【図29】

暗号化発券情報のフォーマットを示す図である。

【図30】

復号処理を説明するためのフローチャートである。

【図31】

従来のICカードの流通を説明するための図である。

【図32】

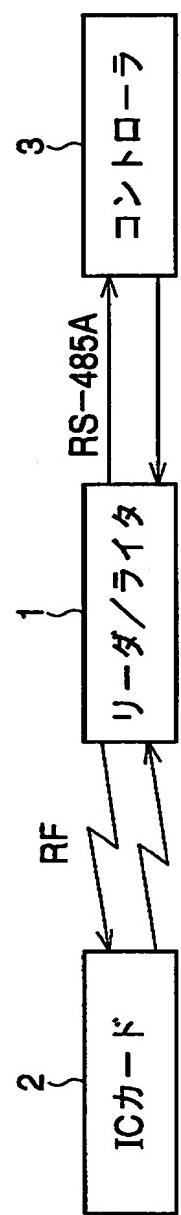
従来のICカードの流通を説明するための図である。

【符号の説明】

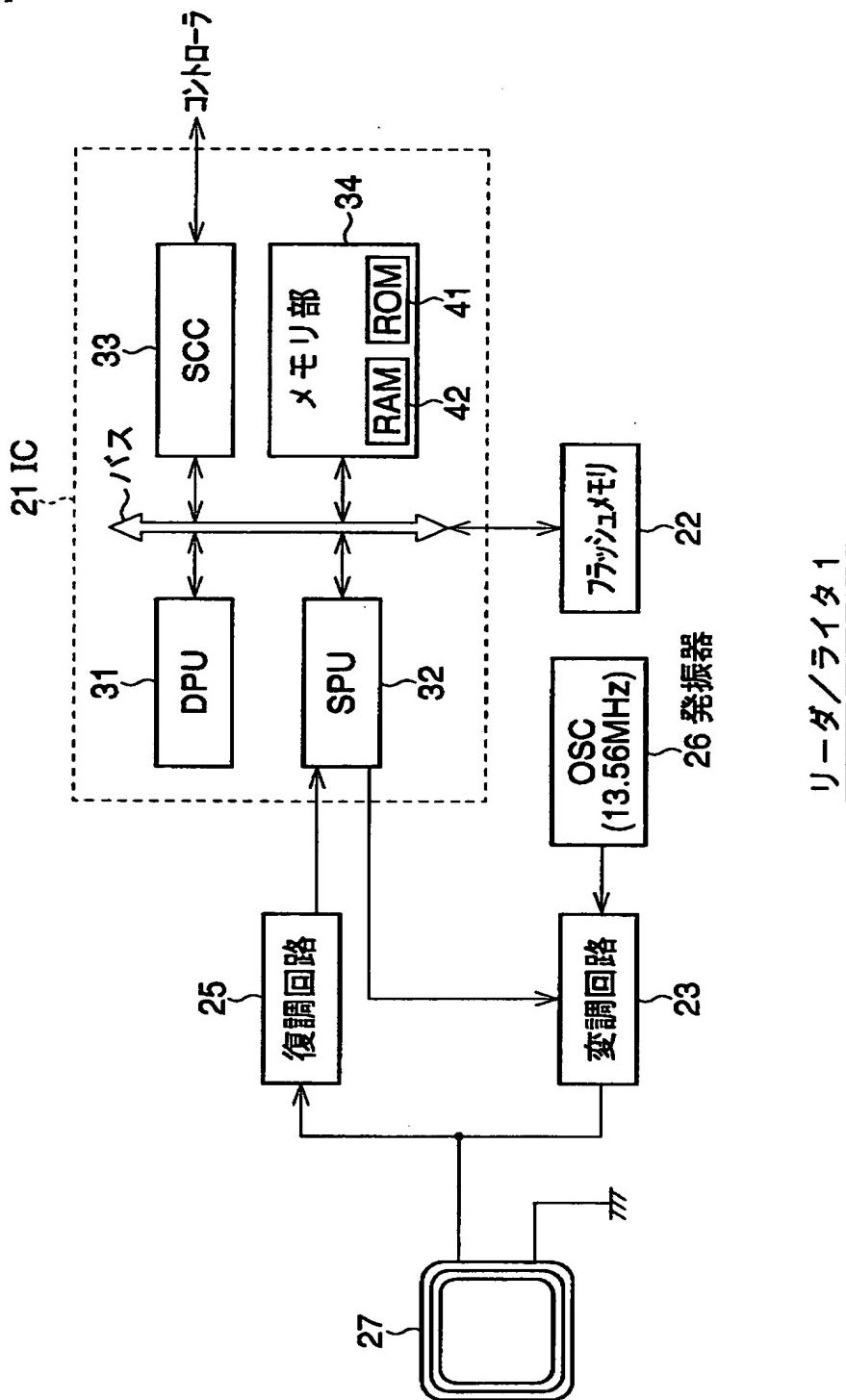
- 1 リーダ／ライタ, 2 ICカード, 3 コントローラ, 21 IC,  
, 23 変調回路, 25 復調回路, 27 アンテナ, 51 IC,  
52 コンデンサ, 53 アンテナ, 61 RFインターフェース部, 62  
BPSK復調回路, 63 PLL部, 64 演算部, 65 ROM,  
66 EEPROM, 67 RAM, 68 BPSK変調回路, 81 ASK  
SK復調部, 82 電圧レギュレータ, 83 発振回路, 84 ASK変  
調部, 91 シーケンサ, 92 暗号／復号部, 93 パリティ演算部,  
101 発券機, 111 サービス提供装置, 121 伝送媒体, 13  
1 発券情報提供装置

【書類名】図面

【図1】

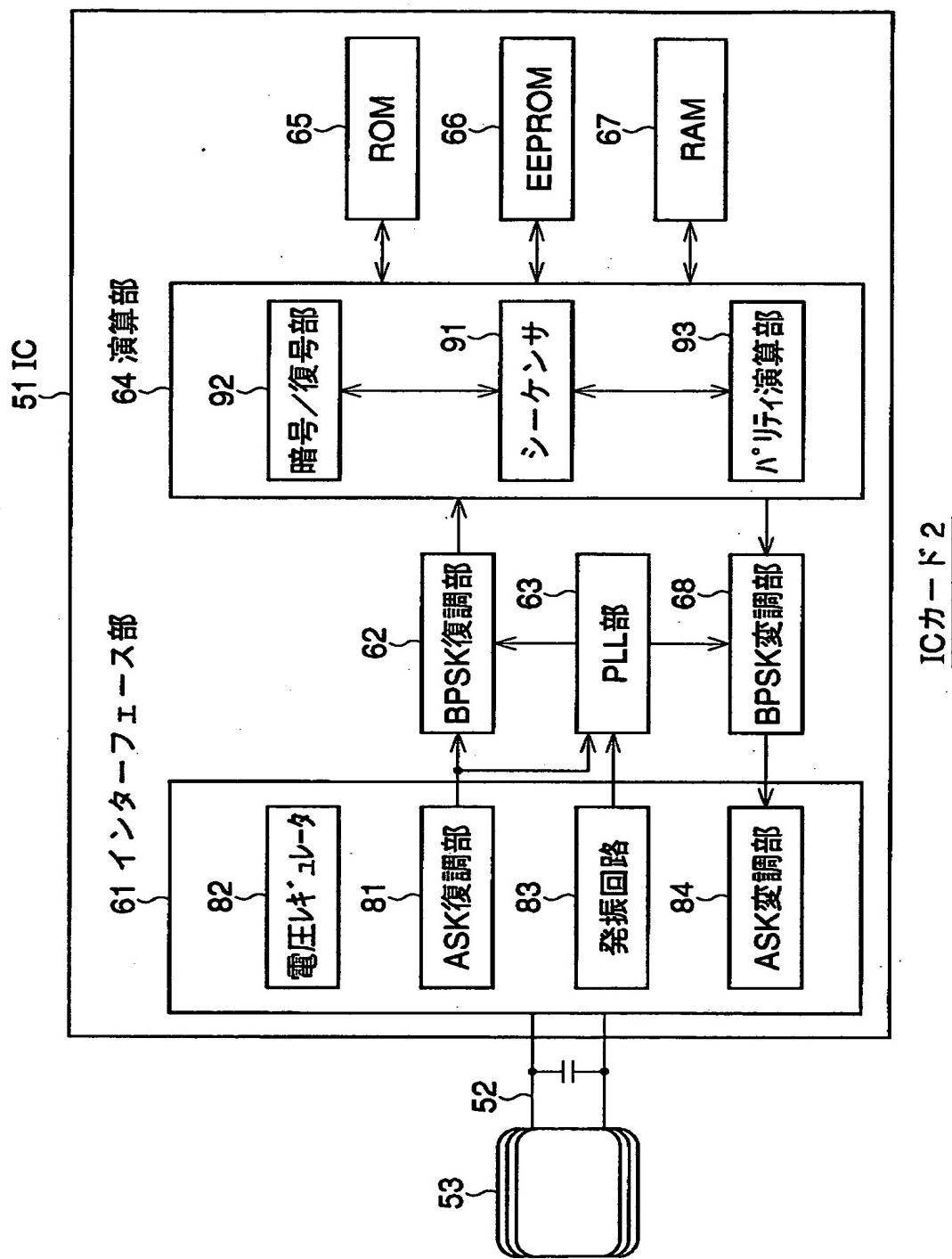


【図2】

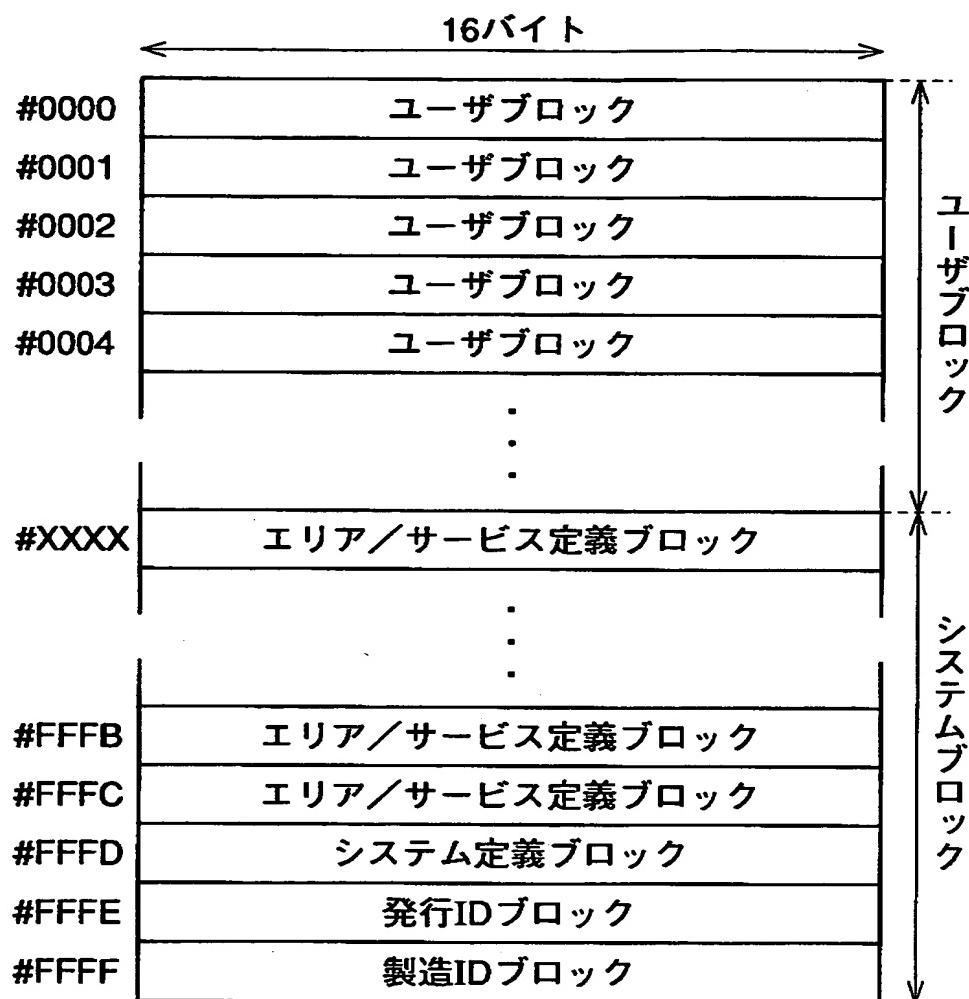


リーダ/ライタ1

【図3】

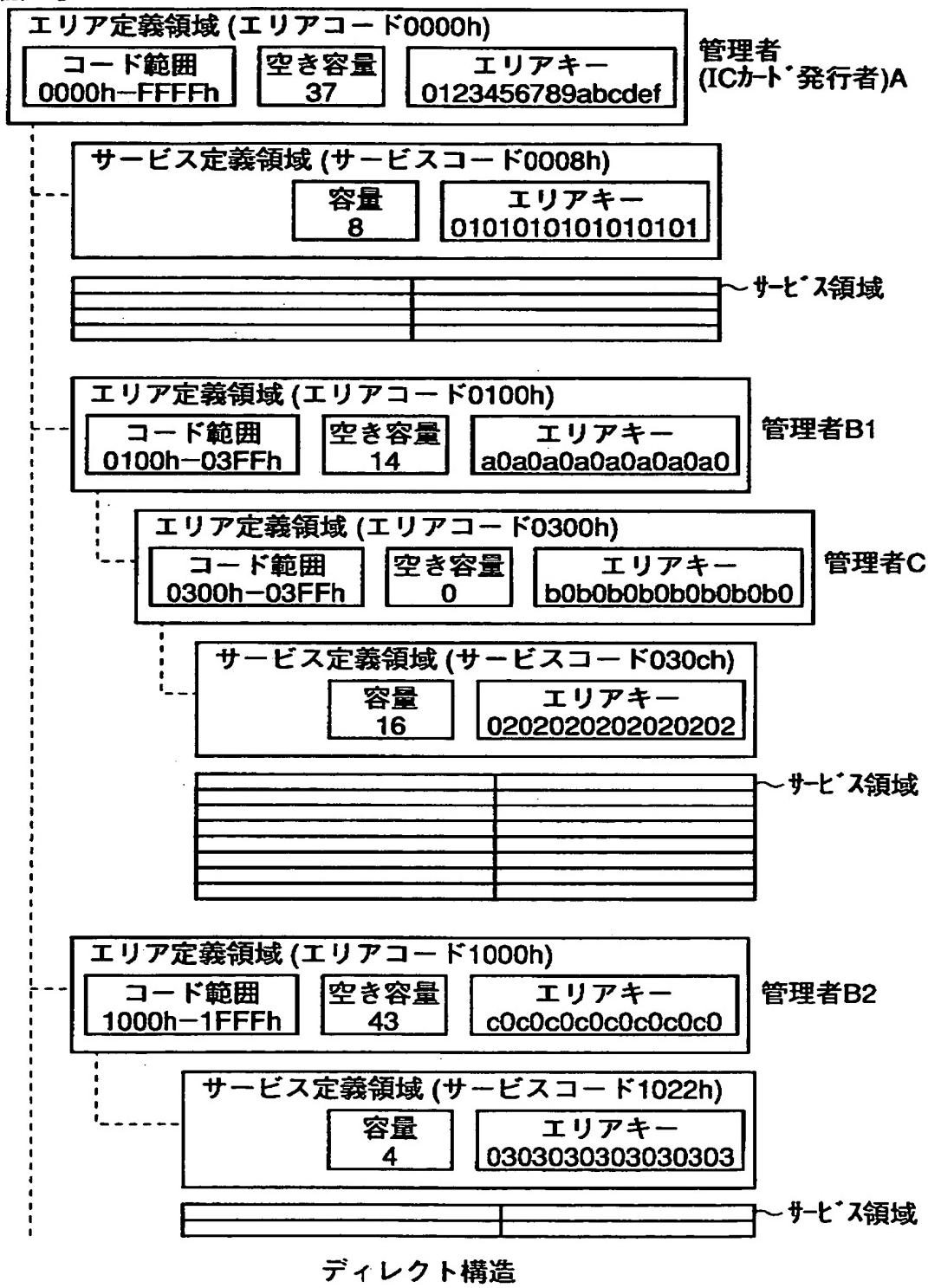


【図4】

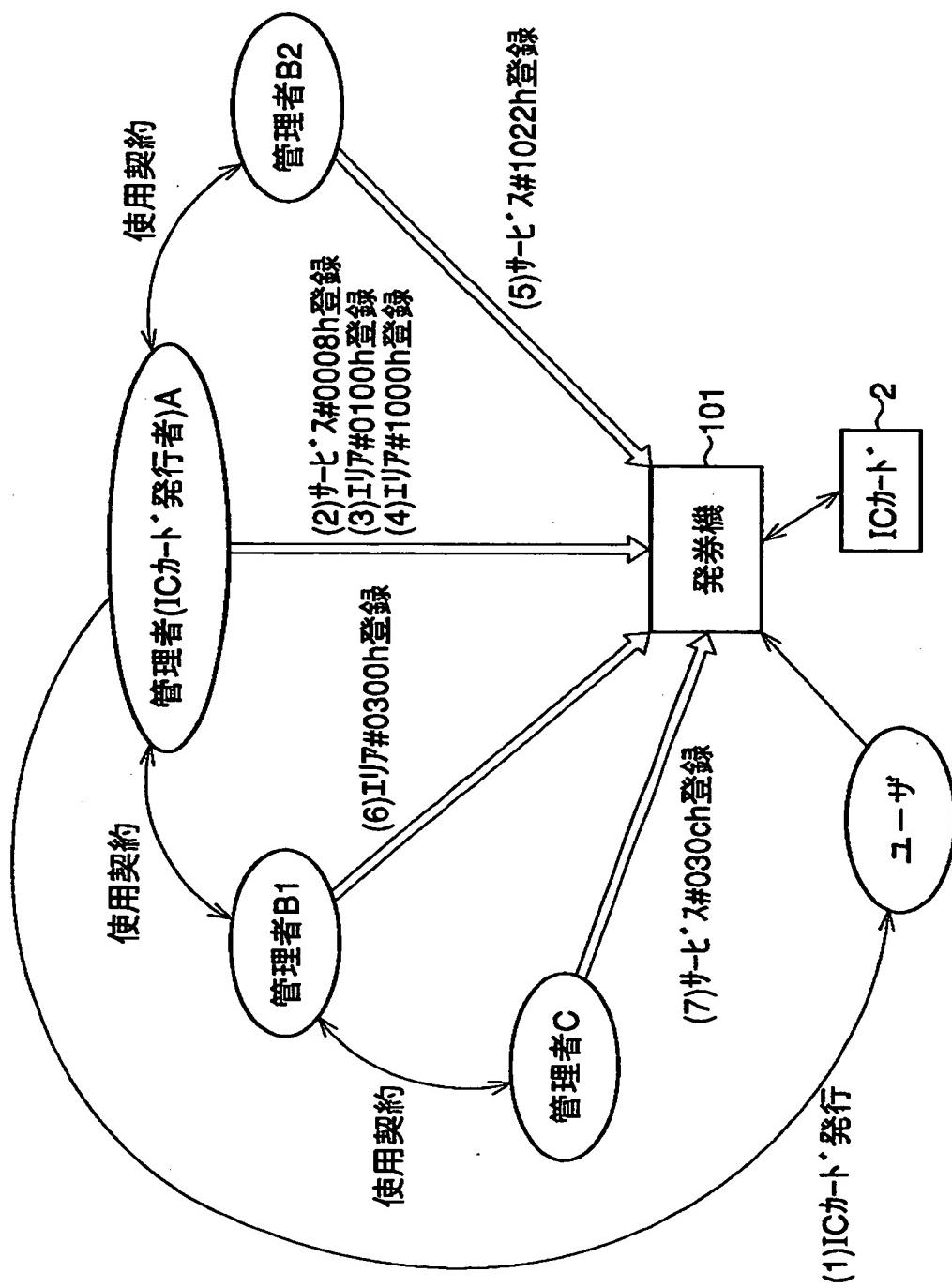


EEPROM66の論理フォーマット

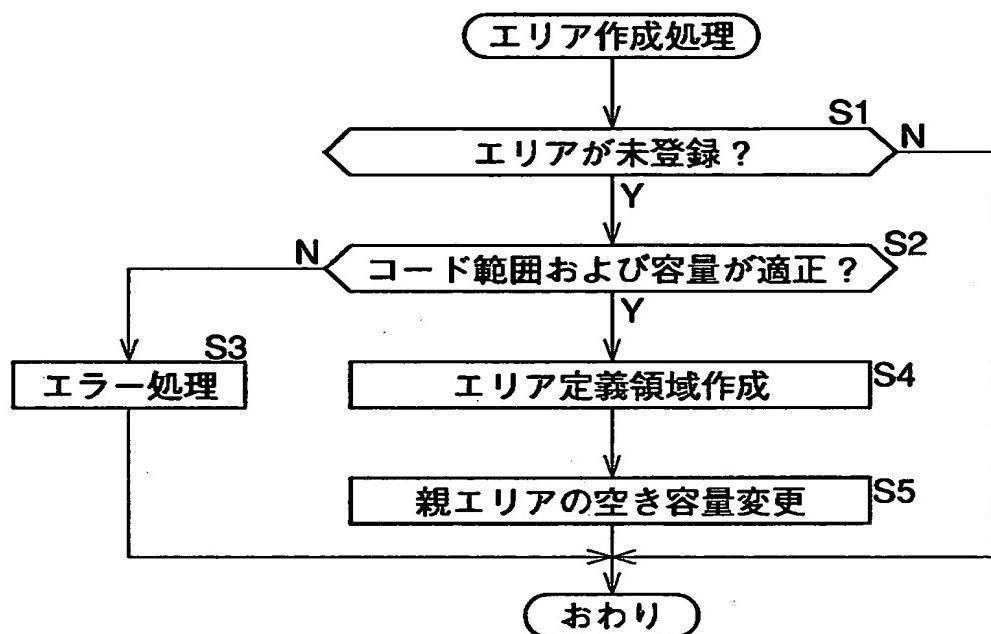
【図5】



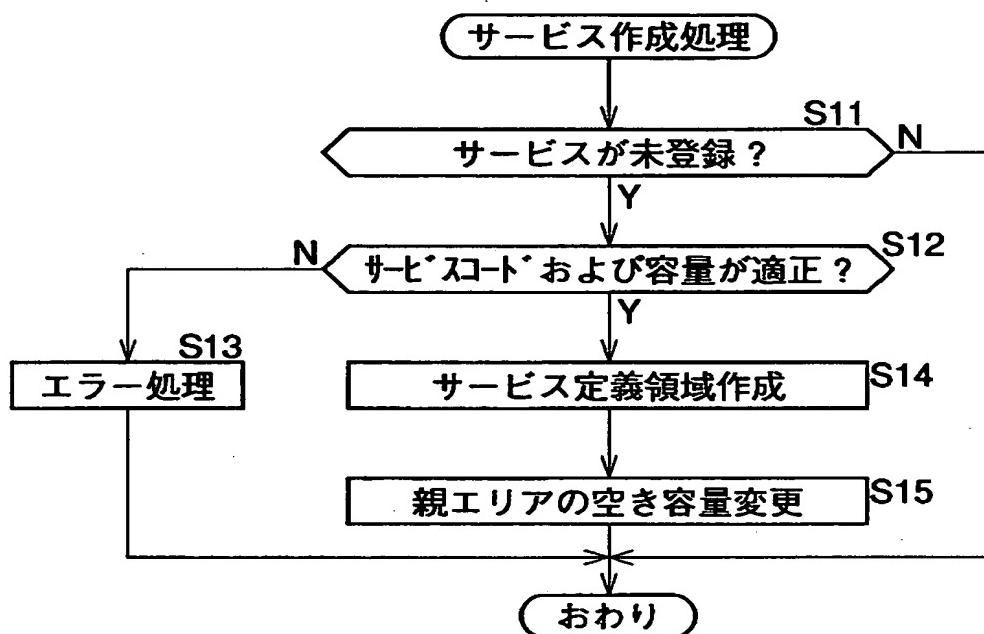
【図6】



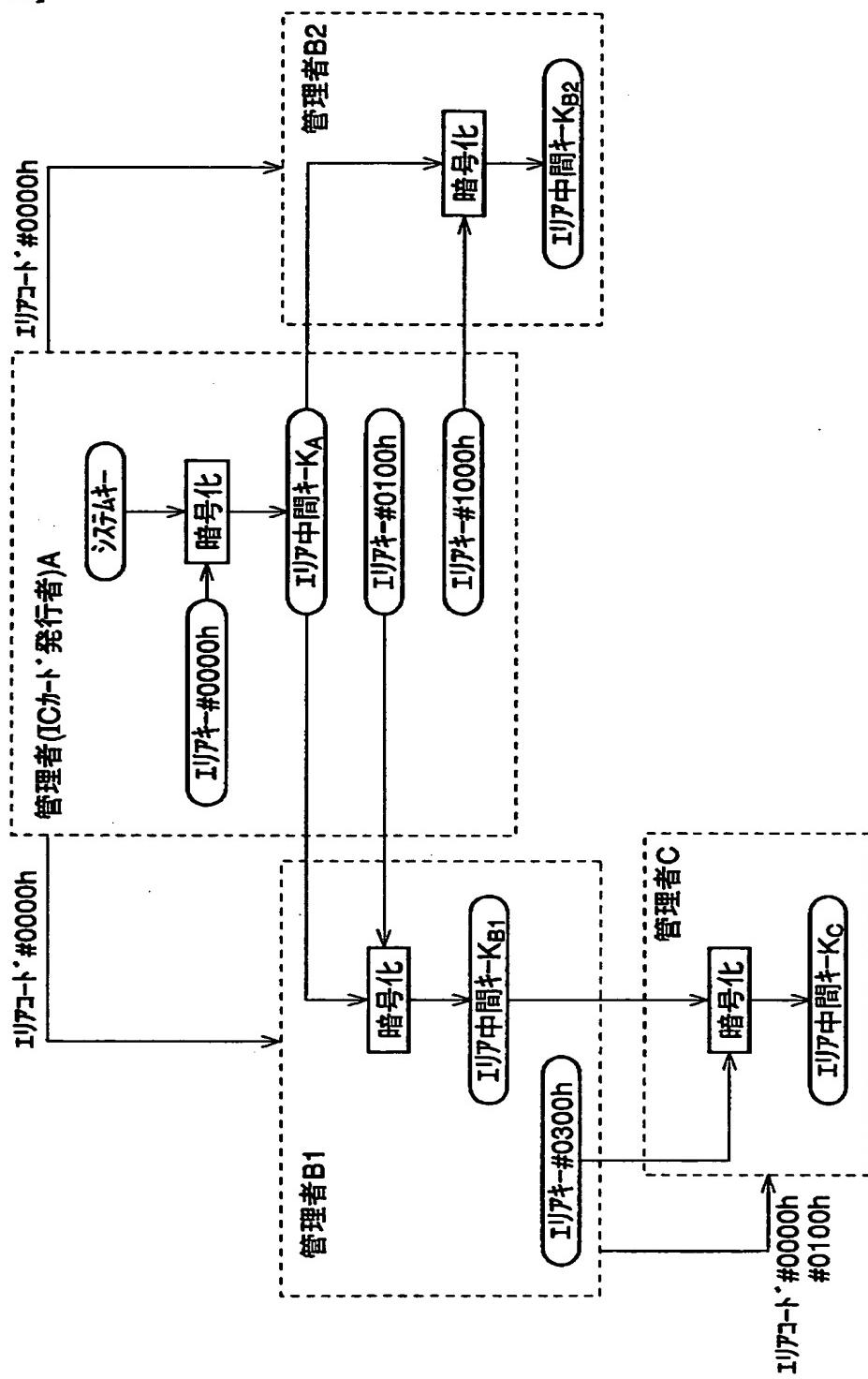
【図7】



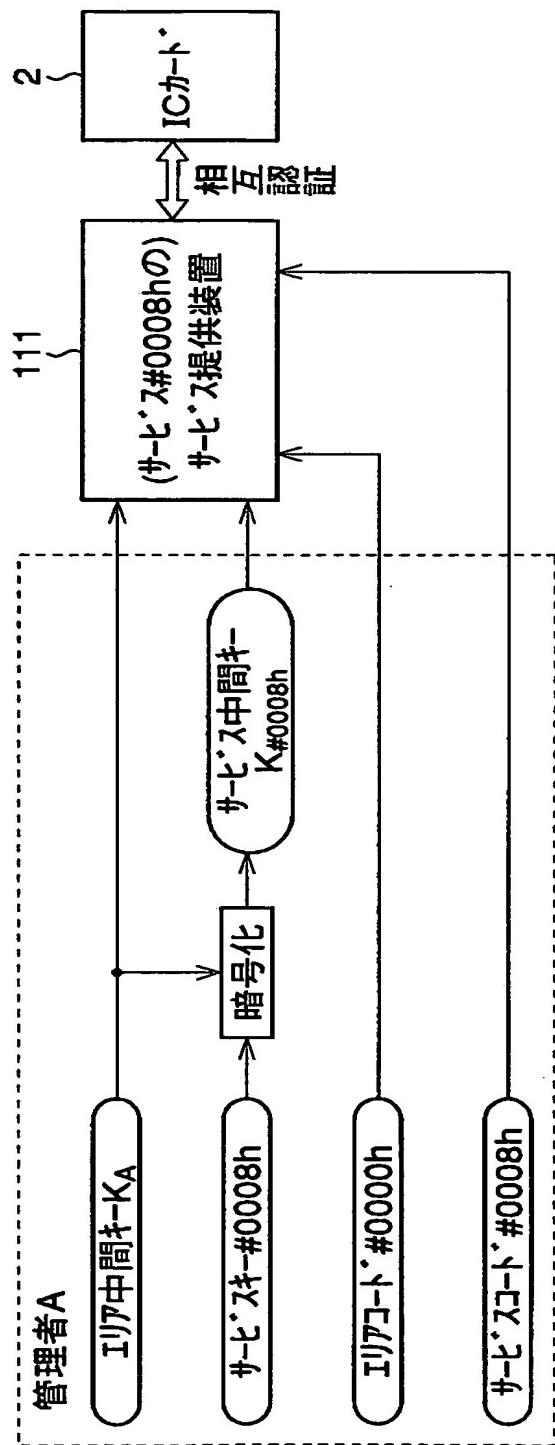
【図8】



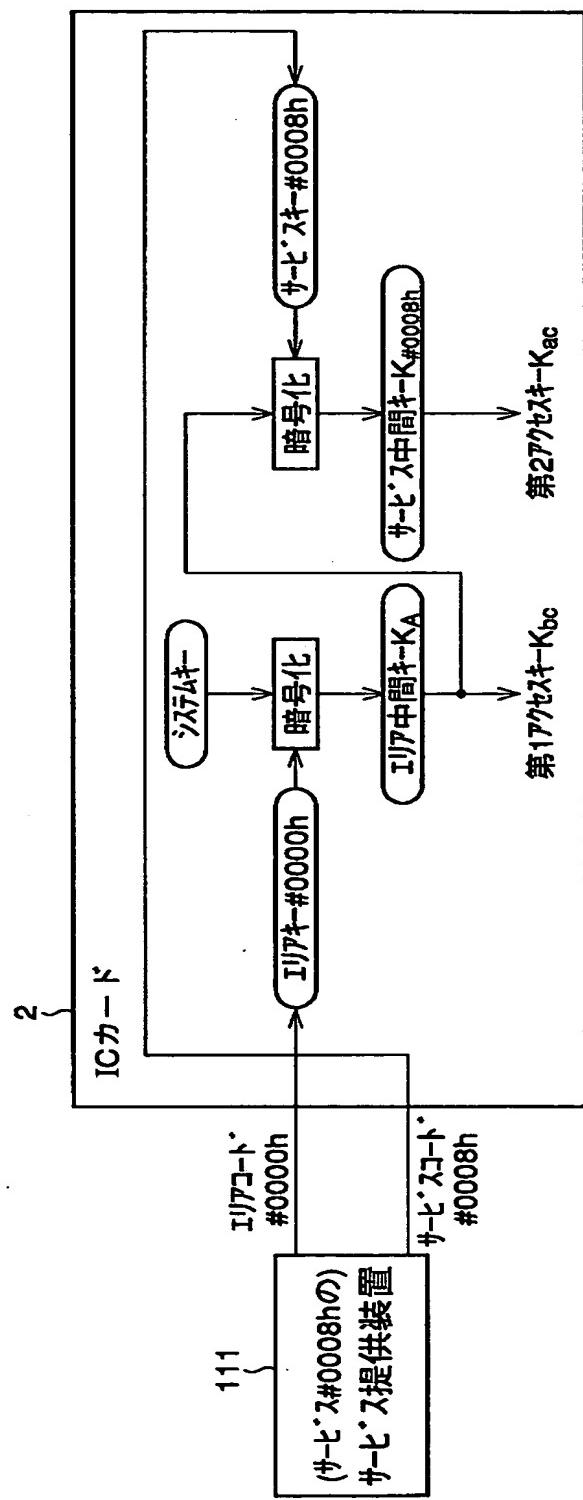
【図9】



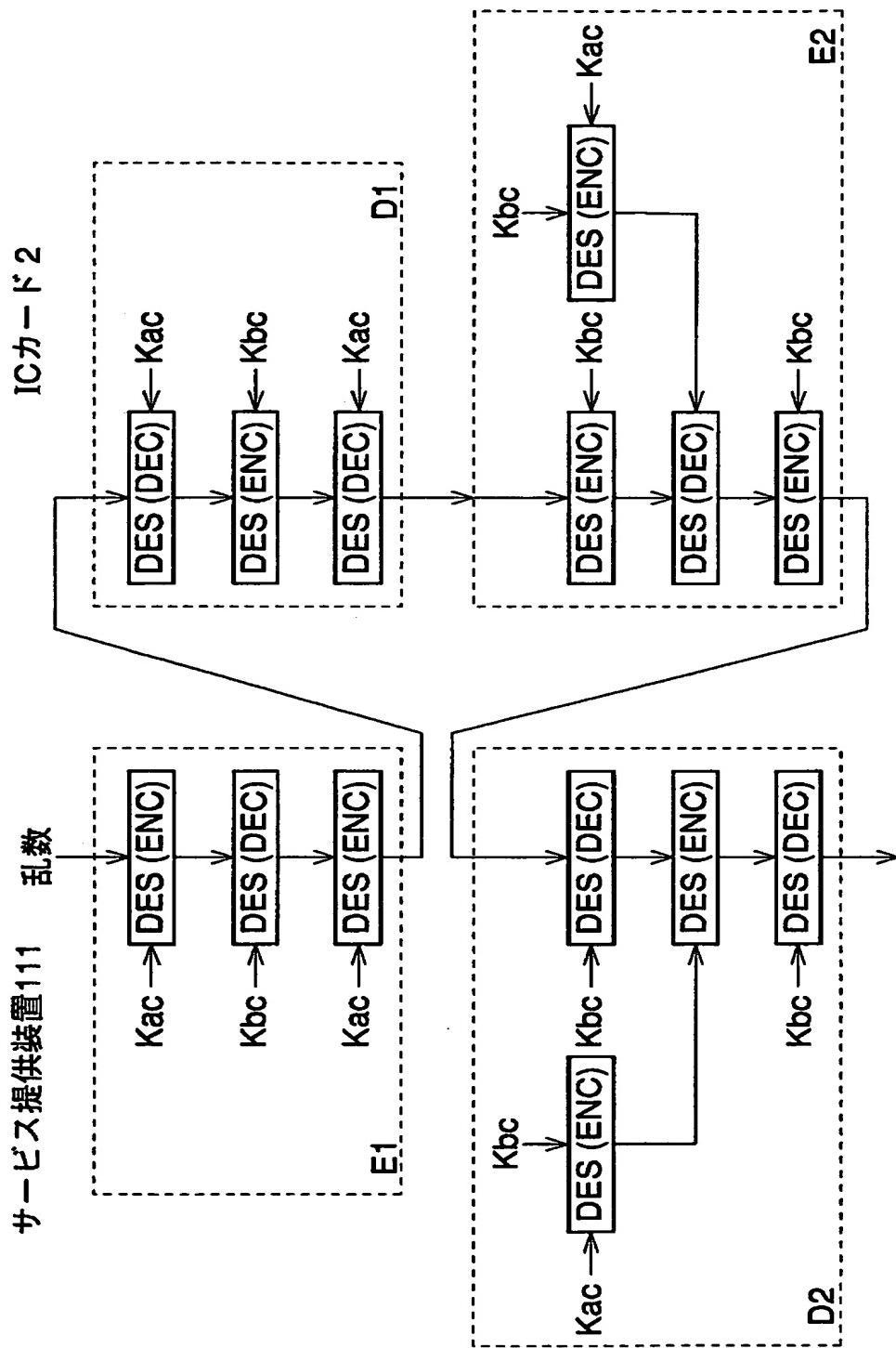
【図10】



【図11】



【図12】

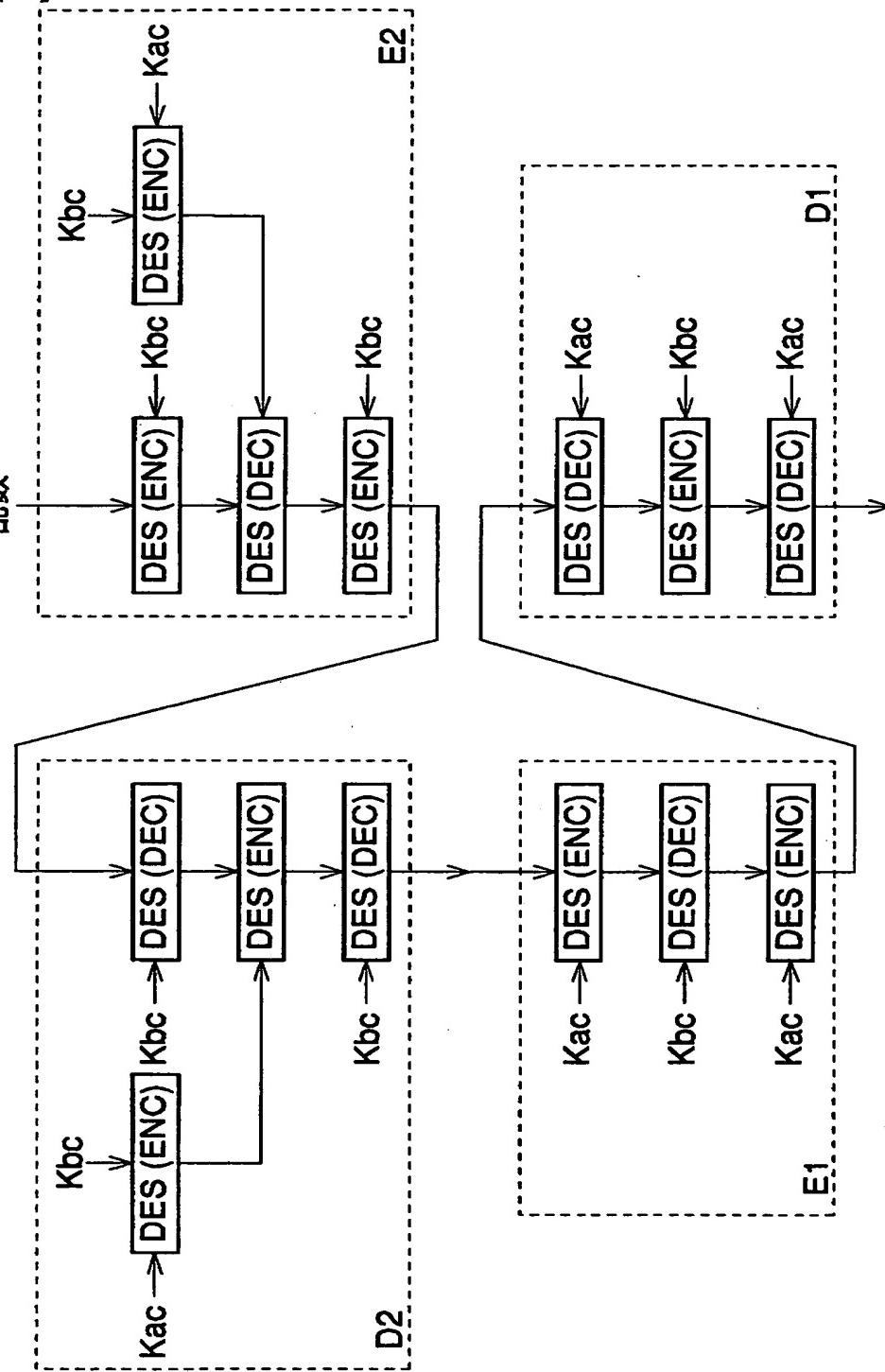


リーダ／ライタからカードの認証

サービス提供装置111

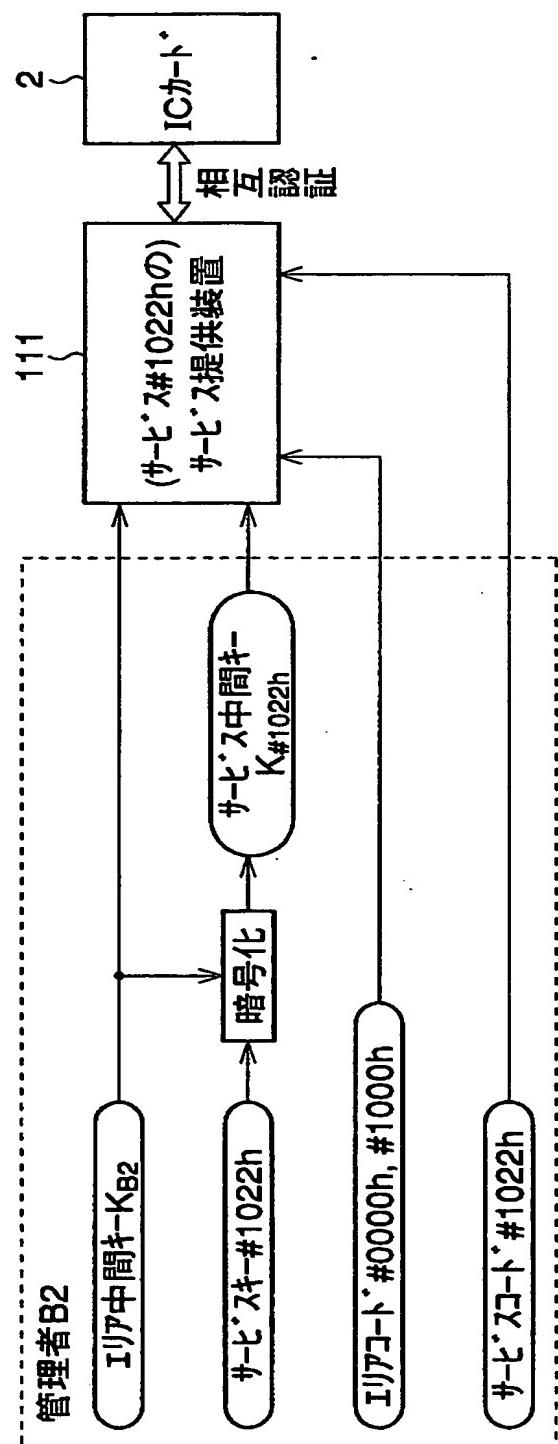
ICカード2

[図13]

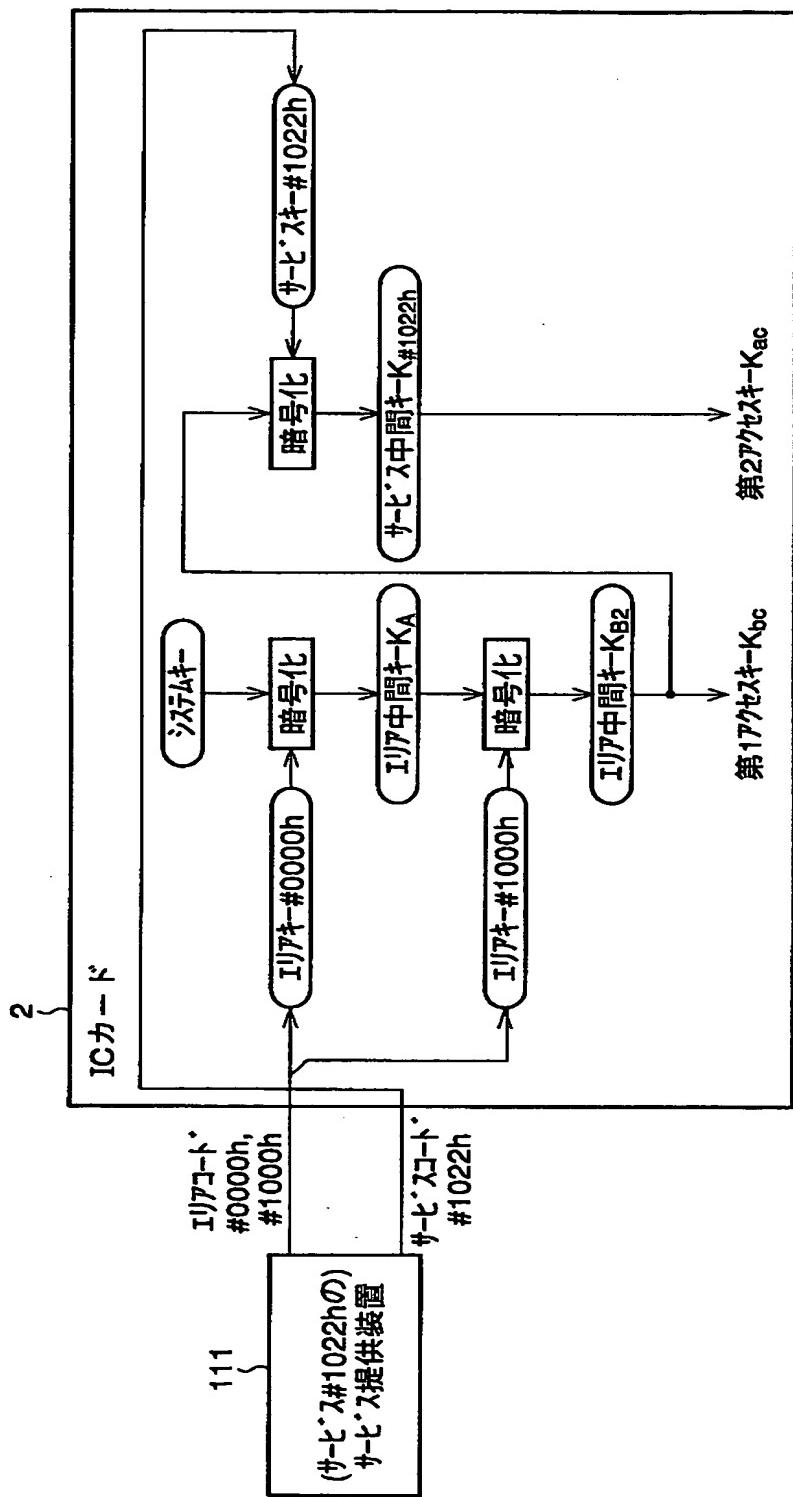


カードからリーダ／ライタの認証

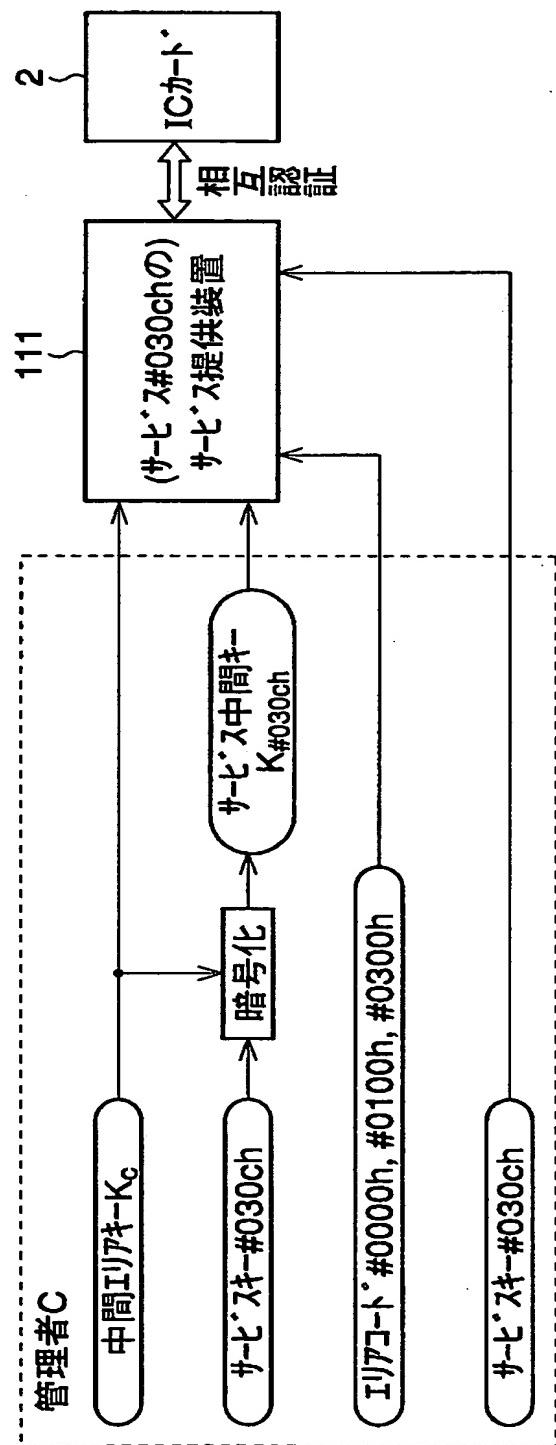
【図14】



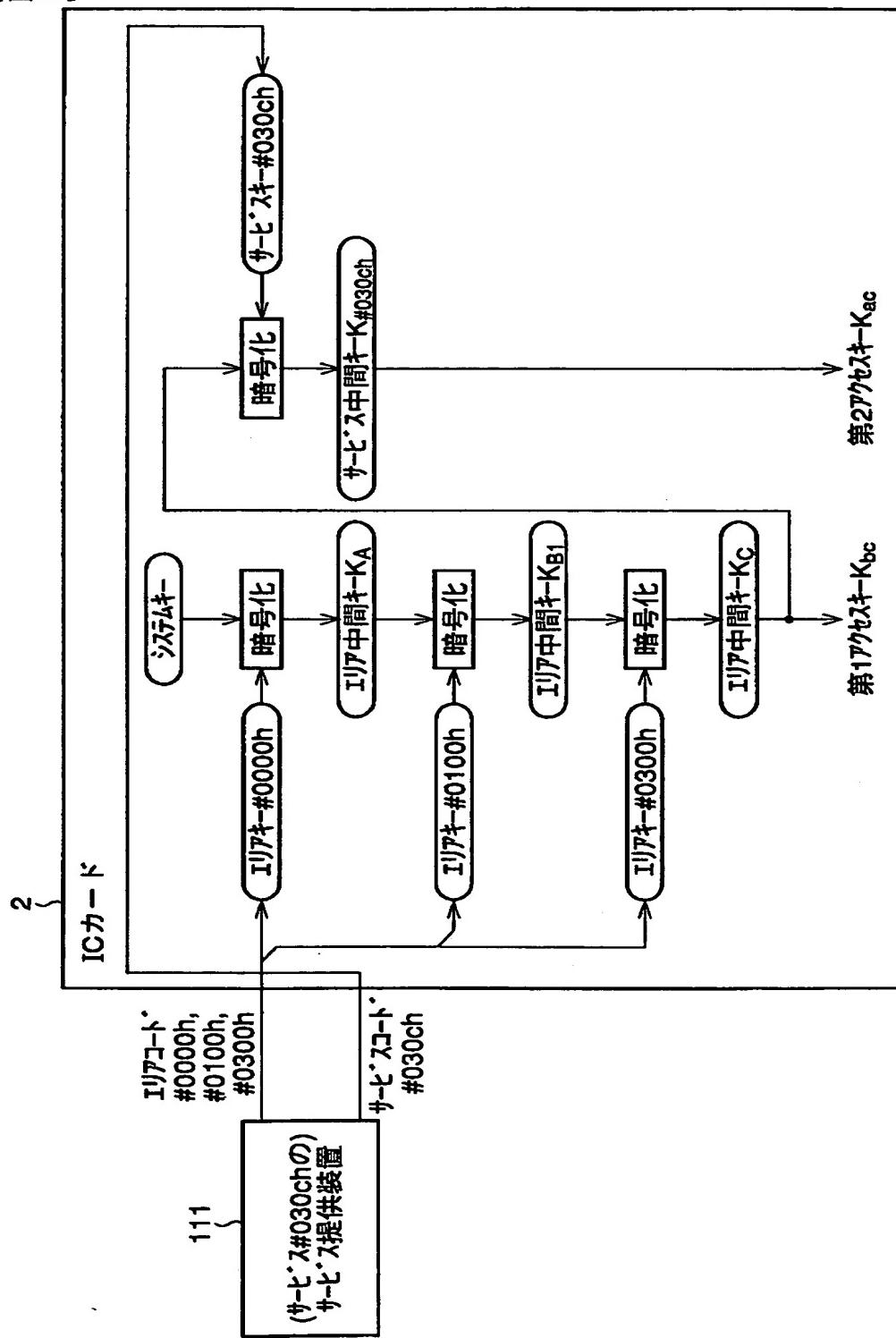
【図15】

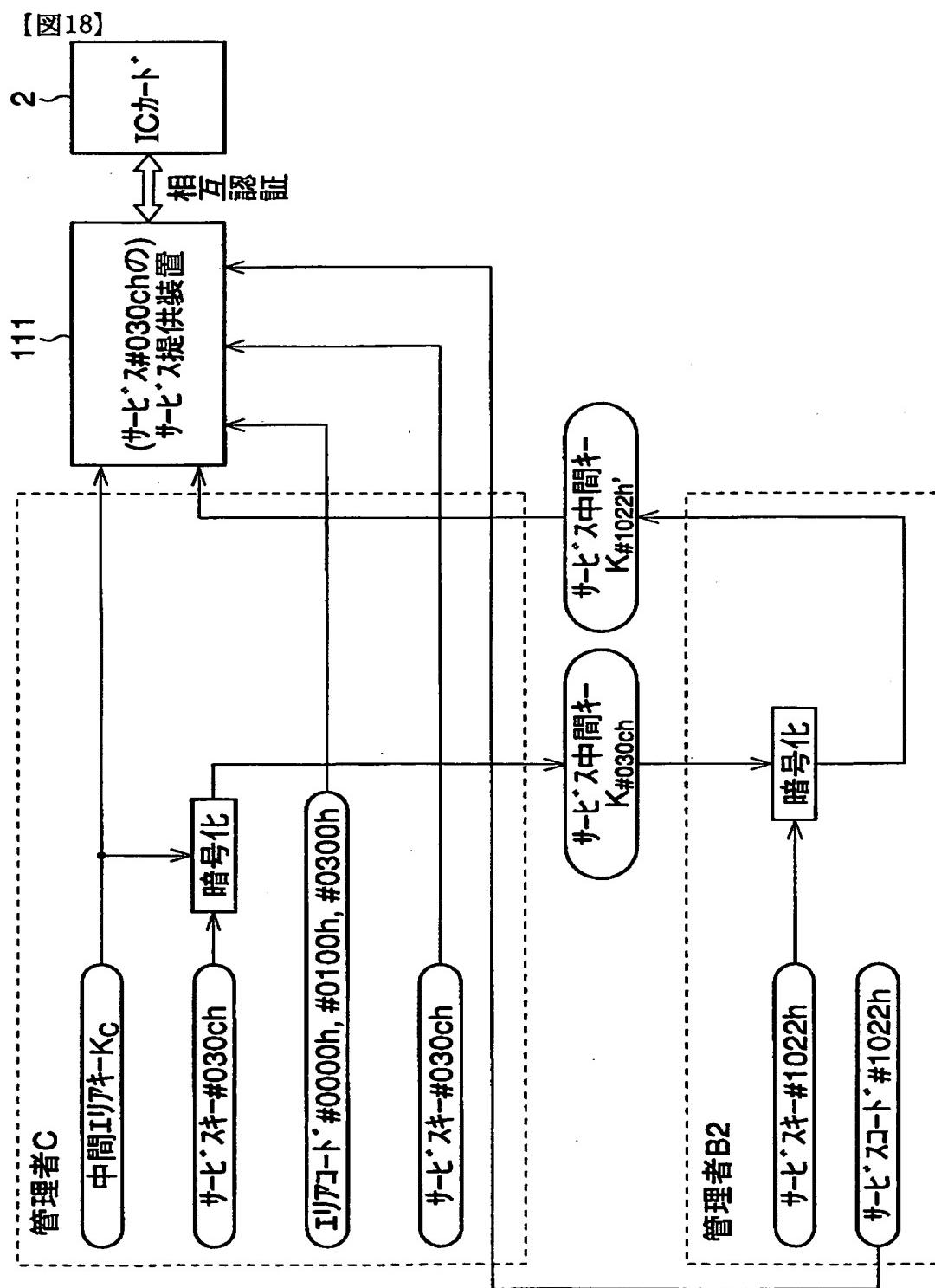


【図16】

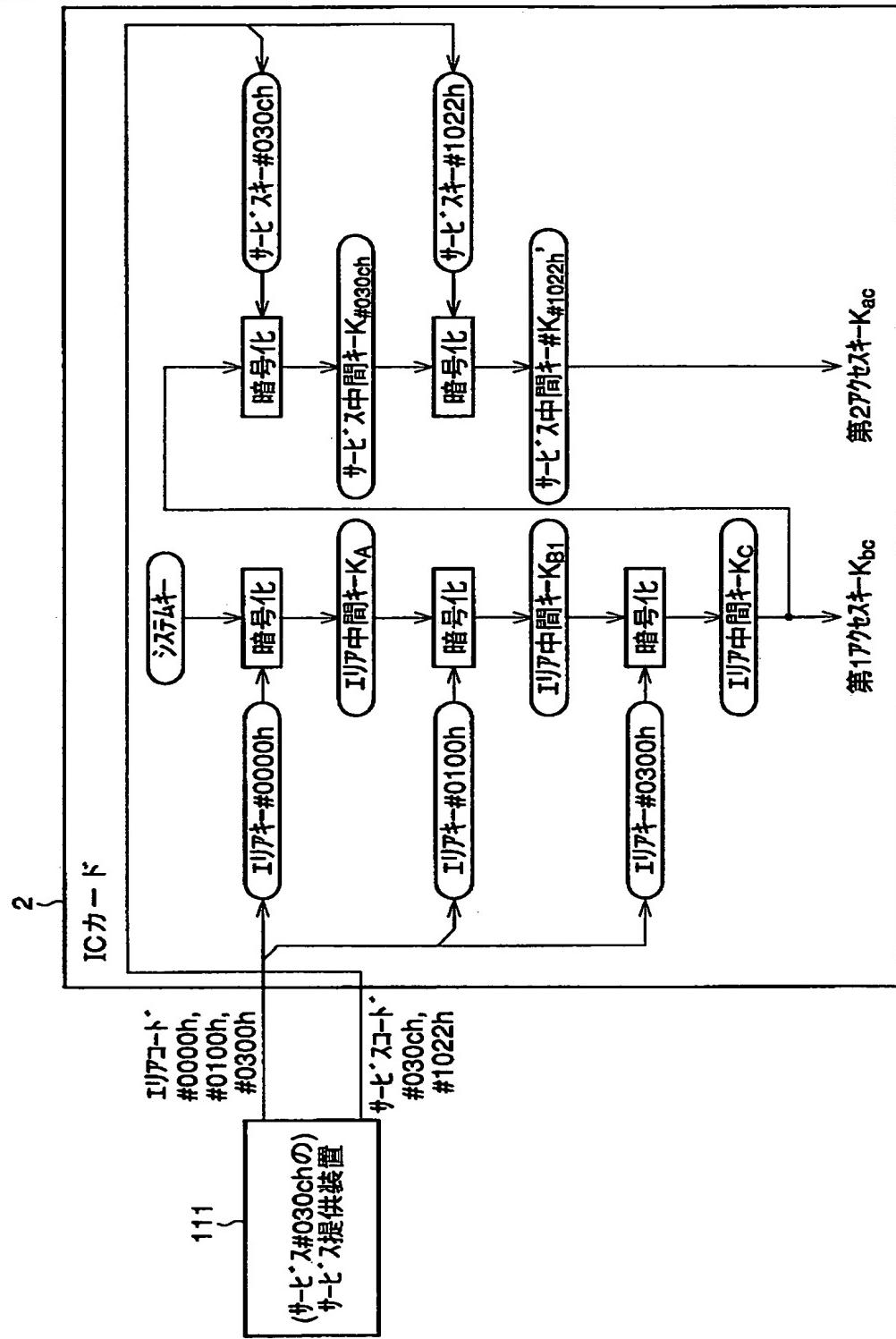


【図17】

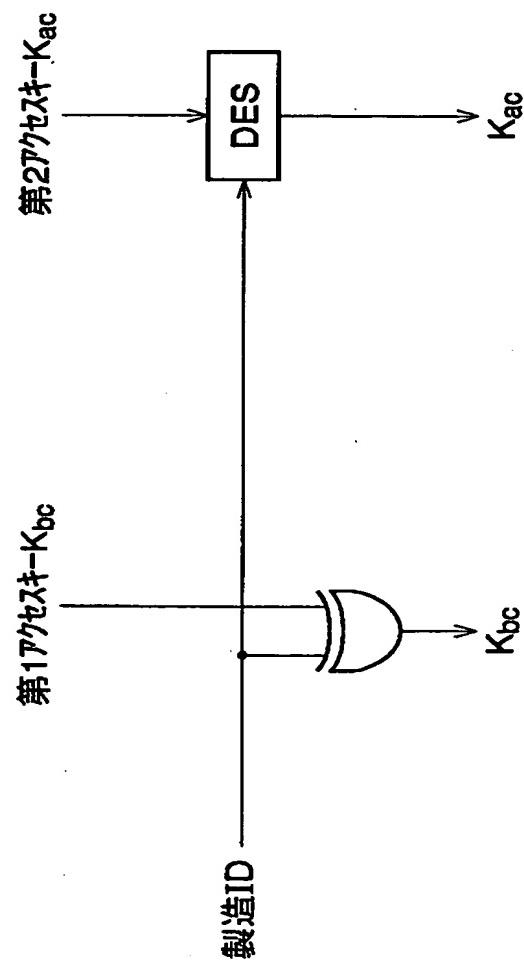




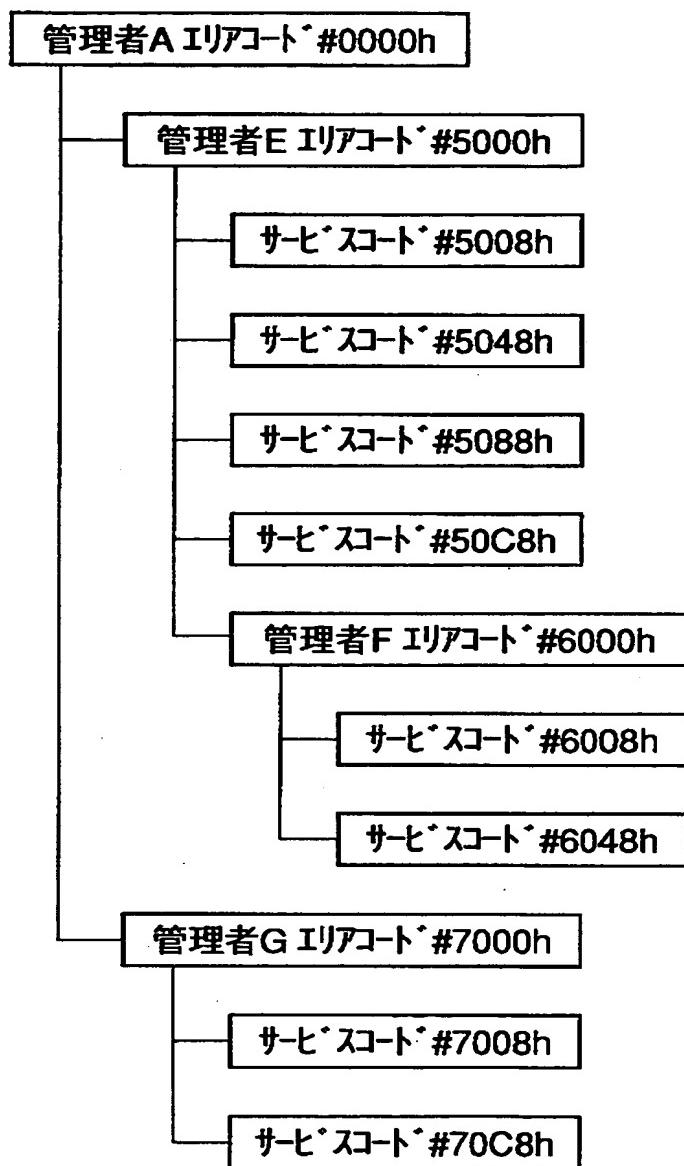
【図19】



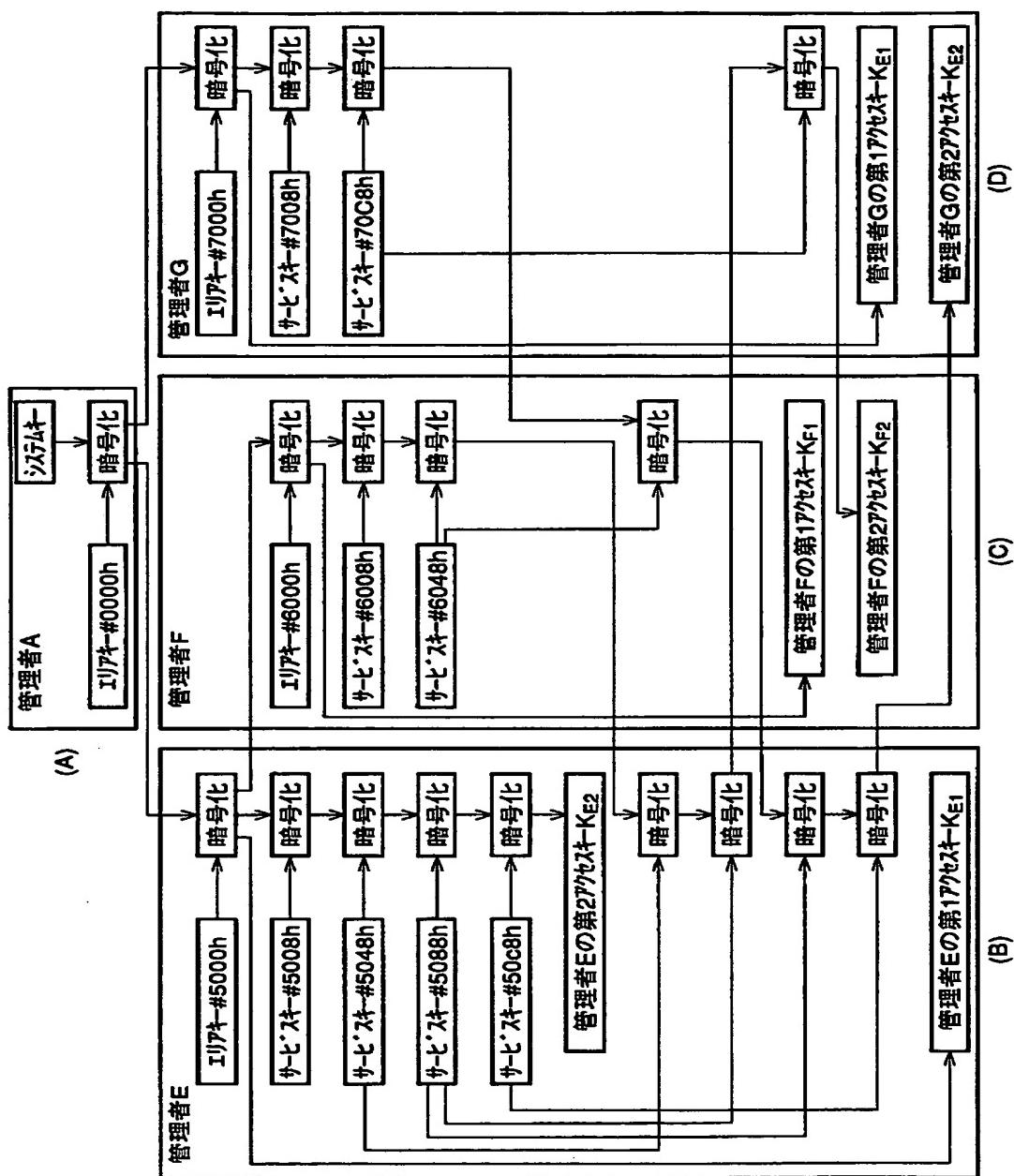
【図20】



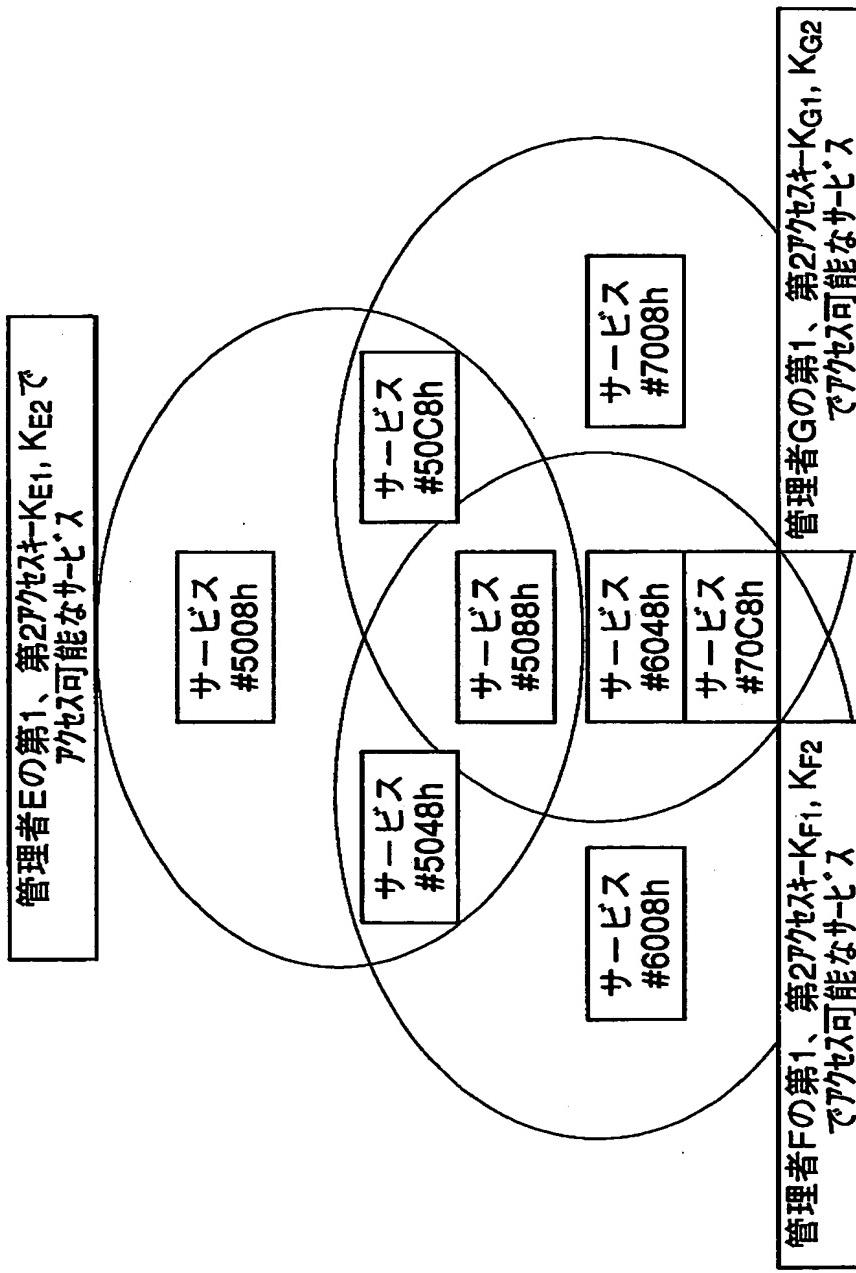
【図21】



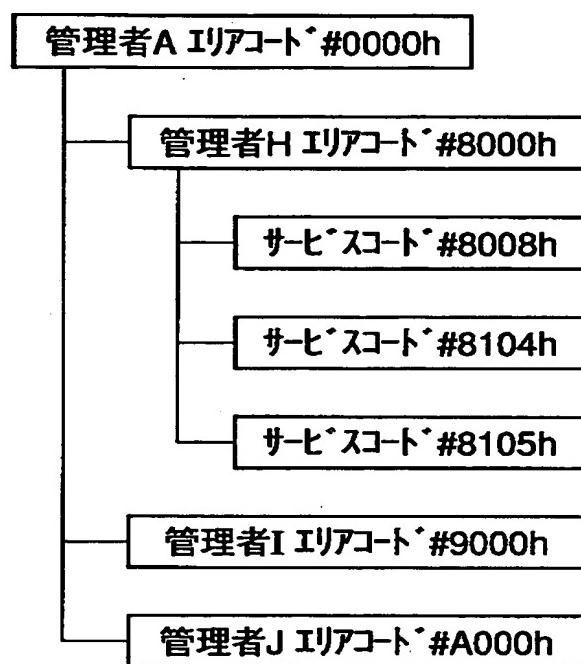
【図22】



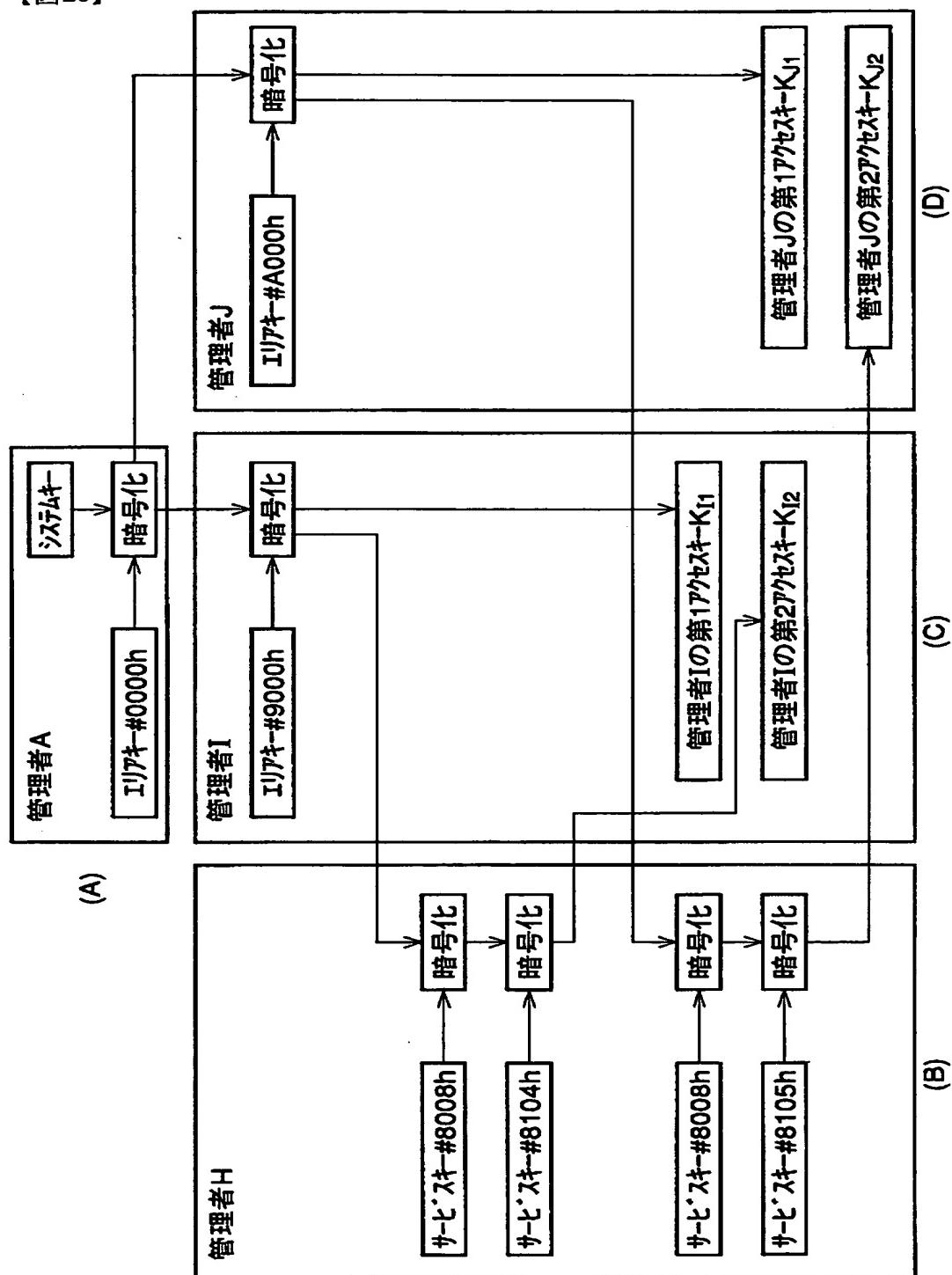
【図23】



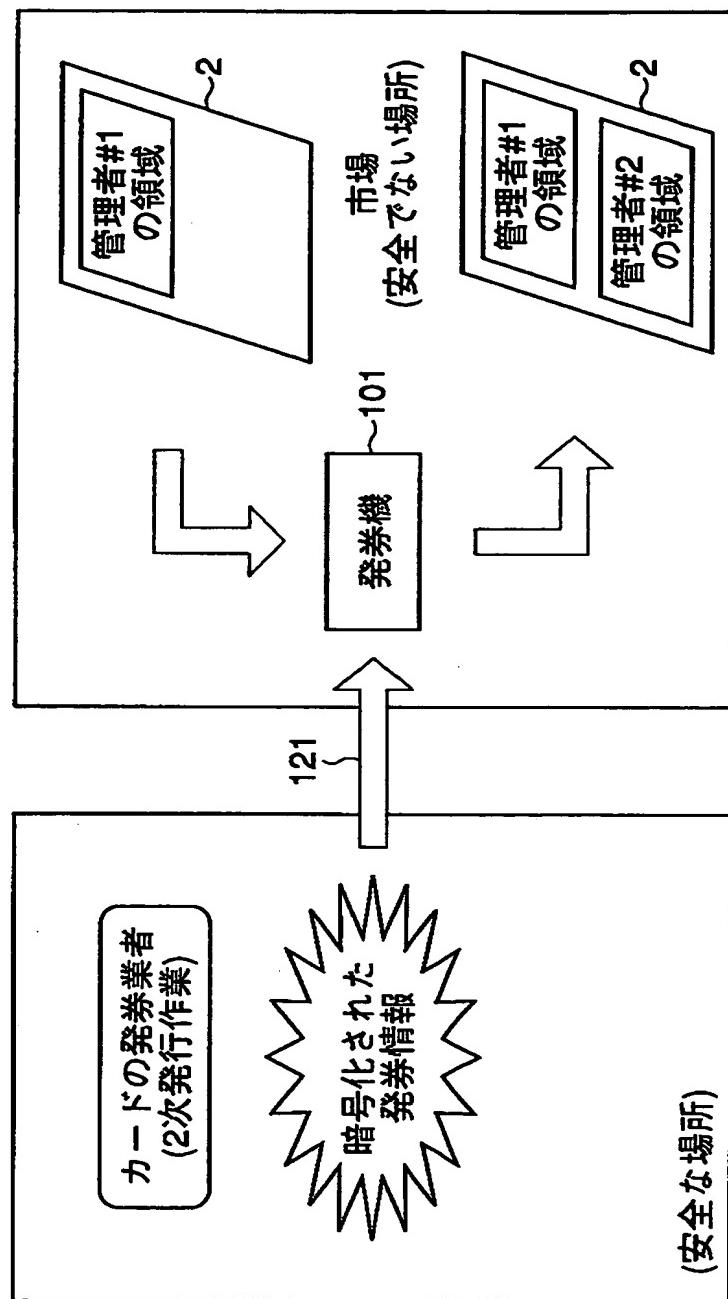
【図24】



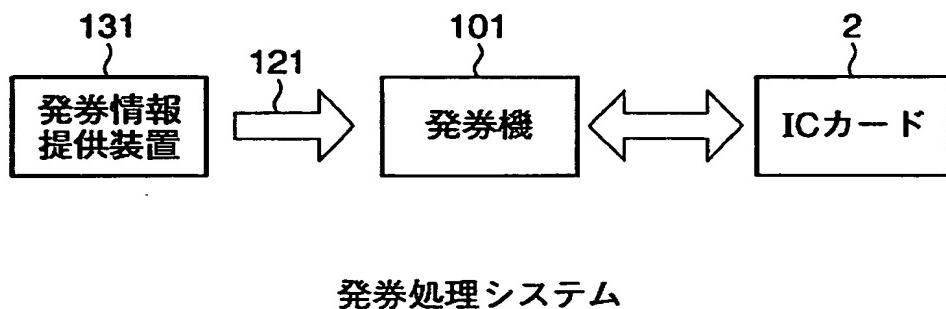
【図25】



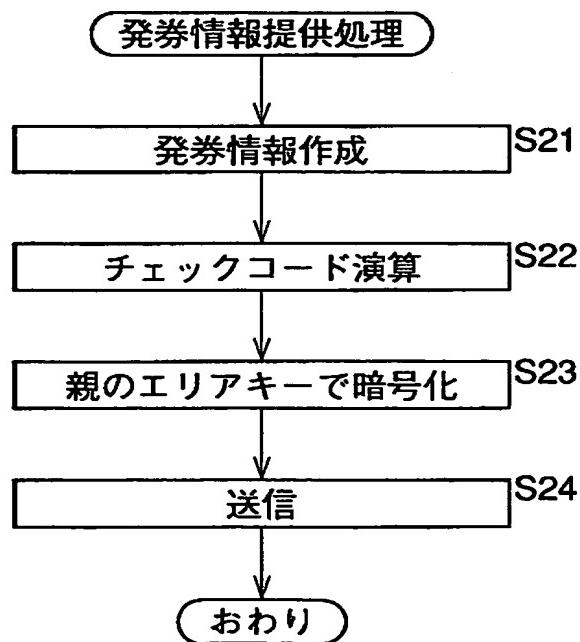
【図26】



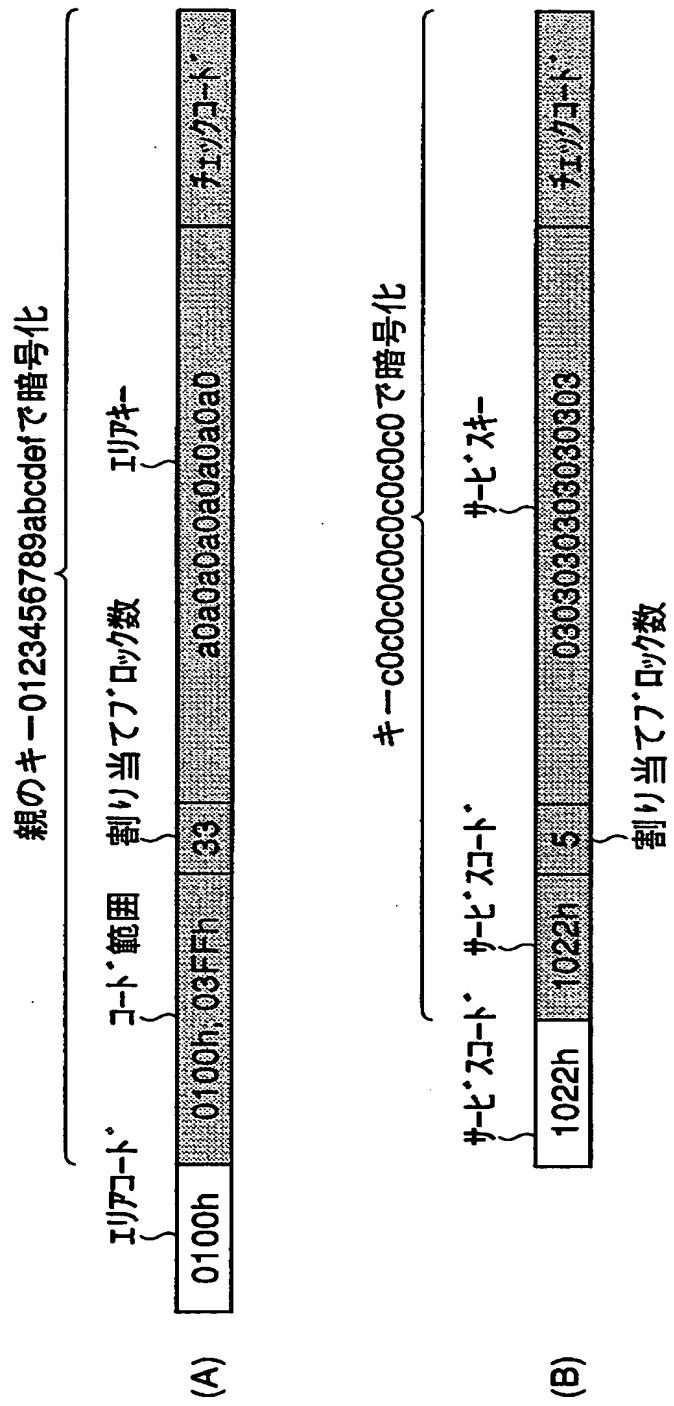
【図27】



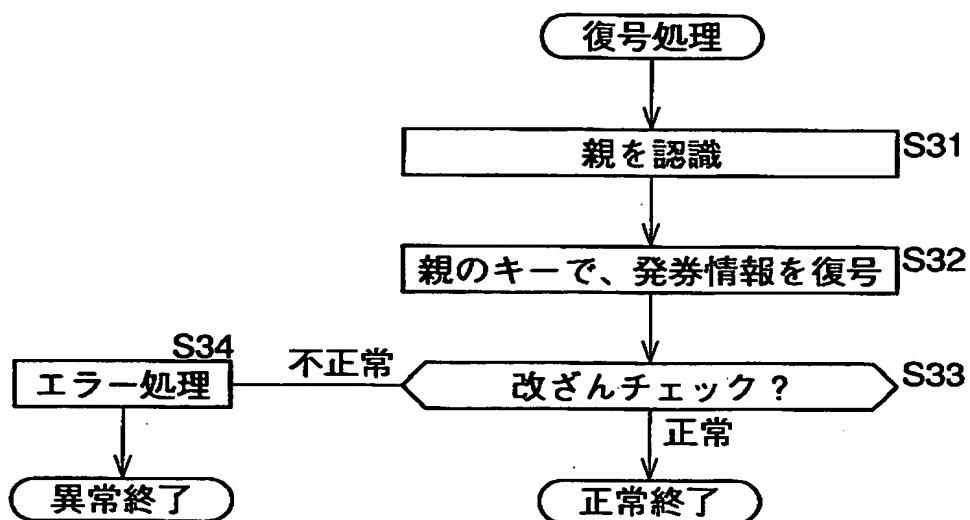
【図28】



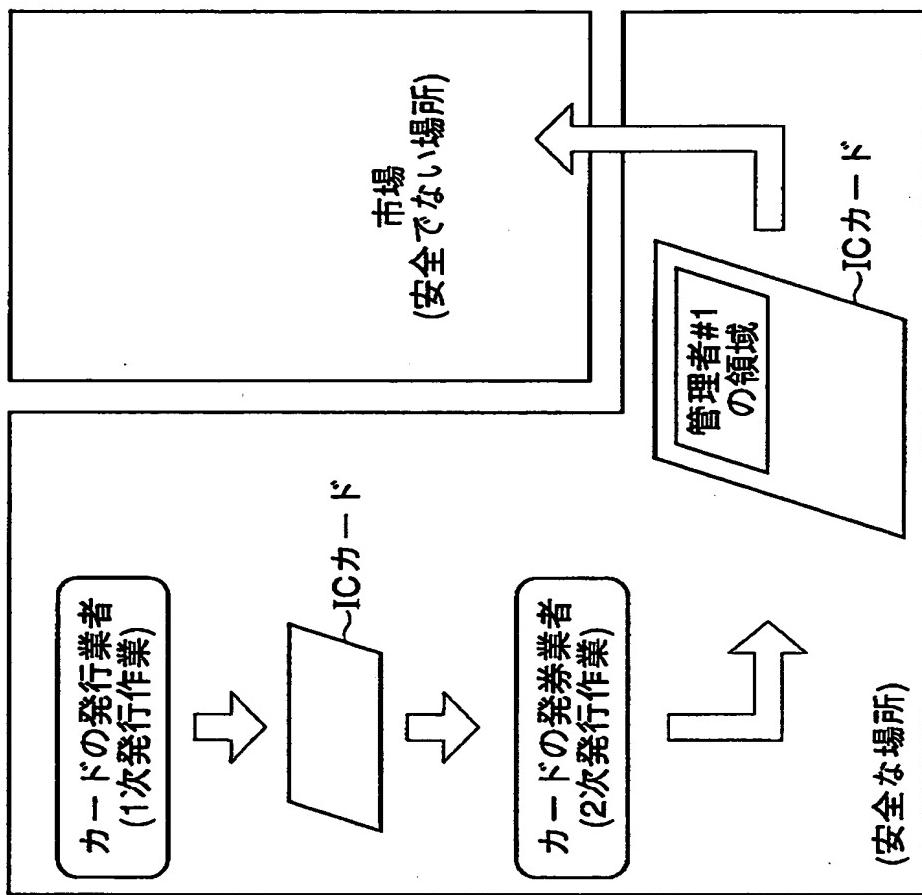
【図29】



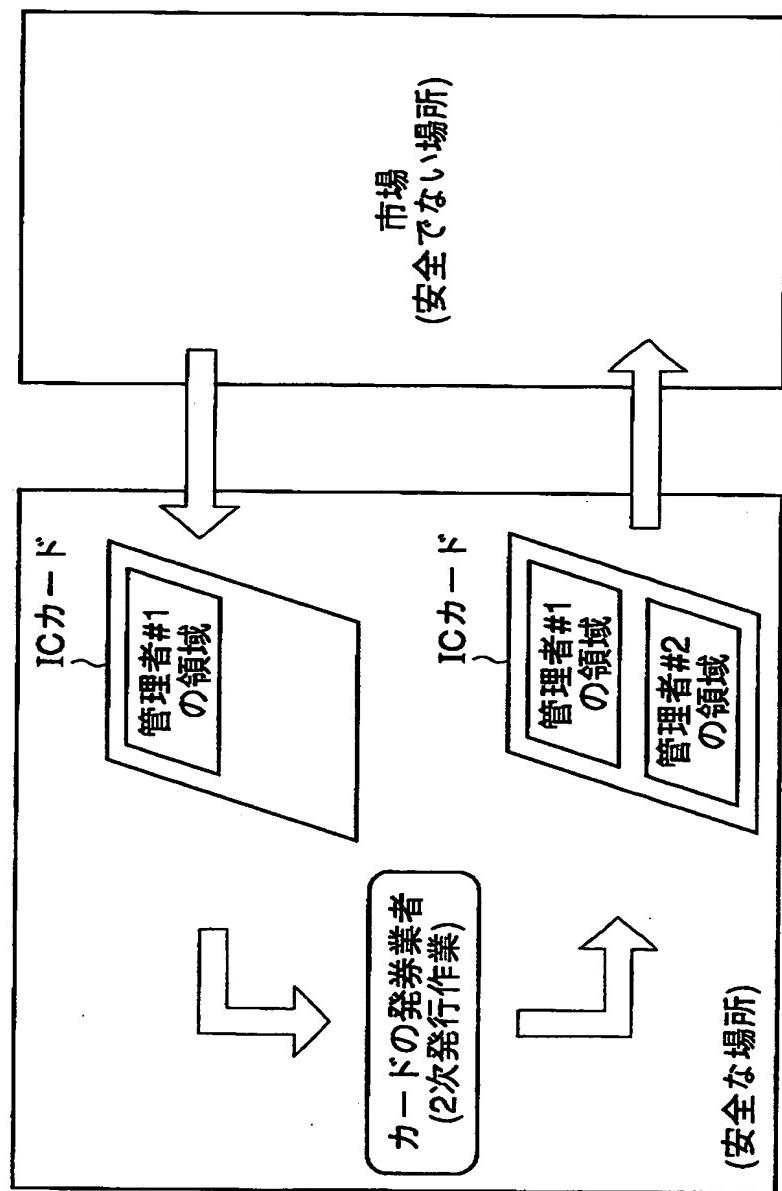
【図30】



【図31】



【図32】



【書類名】 要約書

【要約】

【課題】 ICカードによるサービスの提供を開始するのに、ICカードに記憶させることが必要な発券情報の改竄や盗聴等を防止する。

【解決手段】 発券情報提供装置131では、発券情報が暗号化され、その結果得られる暗号化発券情報が、伝送媒体121を介して、発券機101に送信される。発券機101では、発券情報提供装置131からの暗号化発券情報が受信されて登録される。そして、発券機101は、ICカード2と通信可能な状態となると、登録されている暗号化発券情報を、ICカード2に送信する。ICカード2では、発券機101からの暗号化発券情報が復号され、その結果得られる発券情報が記憶される。

【選択図】 図27

【書類名】 職権訂正データ  
【訂正書類】 特許願

<認定情報・付加情報>

【特許出願人】

【識別番号】 000002185

【住所又は居所】 東京都品川区北品川6丁目7番35号

【氏名又は名称】 ソニー株式会社

【代理人】 申請人

【識別番号】 100082131

【住所又は居所】 東京都新宿区西新宿7丁目5番8号 GOWA西新宿ビル6F 稲本国際特許事務所

【氏名又は名称】 稲本 義雄

出願人履歴情報

識別番号 [00002185]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都品川区北品川6丁目7番35号  
氏 名 ソニー株式会社